Central and Eastern European e|Dem and e|Gov Days 2018

Band 331

Hendrik Hansen, Robert Müller-Török, András Nemeslaki,
Alexander Prosser, Dona Scola, Tamás Szádeczky

Central and Eastern European e|Dem and e|Gov Days 2018

Conference Proceedings

facultas

Austrian Computer Society 2018

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Permalink: http://ejournals.facultas.at

Satz: Österreichische Computer Gesellschaft
Druck: Facultas Verlags- und Buchhandels AG
Printed in Austria
ISBN (facultas Verlag): 978-3-7089-1737-5
ISBN (Österreichische Computer Gesellschaft): 978-3-903035-20-1
ISSN (Österreichische Computer Gesellschaft): 2520-3401
DOI: 10.24989/ocg.v331

Co-Organisers:

www.ocg.at

uni-nke.hu

www.andrassyuni.eu

www.hs-ludwigsburg.de

www.idsi.md

Partners:

www.okfbudapest.hu

www.kas.de

Sponsors:

www.bwstiftung.de

Gefördert von der BW STIFTUNG Baden-Württemberg

www.austrian.com

TABLE OF CONTENTS

DOI: 10.24989/ocg.v331.0

PREFACE

DOI: 10.24989/ocg.v331.1

The Smart Cities concept is the special theme of this year's conference, as it is a focal point for a number of digital government initiatives. First and foremost it requires state-of-the-art citizen interaction in mobile- and web-based services as well as a widely-accepted electronic ID. The ID should also be useable via mobile devices and not only via a "classical" web interface from stationary PCs. Without this base line, there is no meaningful interface to the citizen.

However, the smart city concept also hinges on the feedback loop from decentral entities, such as sensors (and to a lesser degree actuators) and human users. They have to be connected to a city- or region-wide network providing input for central data collecting applications ("the cloud"). The ability to perform as a smart city hence also depends on the quality of the technological infrastructure in the city, particularly the Internet of Things. The better the general adoption of such technologies the easier the adoption of the Smart Cities concept.

However, the stream of data collected by the cloud is useless, unless it is analysed and compiled to decision-relevant information. This in turn requires the adoption of methods and technological infrastructure from business analytics, particularly in-memory real-time analytics. Also in this regard, the general maturity of an economy/society/infrastructure in terms of technology adoption considerably helps implement a smart city.

Finally, also conventional eGovernment, as it was adopted in the past decade, still plays a role in back office applications. Electronic files, public procurement, registers etc. are still the backbone for public service provision. Generally, the Smart Cities concept is not only a service provider for citizens and businesses – it is also a yardstick for the infrastructure and technological maturity of a city. In the absence of the necessary infrastructure it may also be the driver for technology adoption and therefore improve a city as a location for doing business in general. May this conference contribute to the better understanding and the exchange of ideas concerning the Smart City.

However, as in the last years, the conference deals with the whole range of the latest developments in the fields of eDemocracy and eGovernment with a special focus on governance in the Danube Region. It aims at analysing innovations in enhancing the quality and efficiency of administrative processes and public services, and in promoting the dialogue and cooperation between politics, administration, civil society and citizen through the use of information technologies. Papers had been solicited in all areas of applying ICT to the Public Sector.

In line with our conference focus on the Danube region, for the first time, we invited a "country of the year" from that region, which presents and critically analyses its achievements in the fields of eDemocracy and eGovernment. The first country selected was Moldova – a country sometimes overlooked both in academic discussions and in practical cooperation among the countries in the Danube region, but highly developed in its digital capacities. Therefore we are happy to welcome a substantial number of papers from Moldovan colleagues in our volume.

The editors of the proceedings volume are most grateful for the support of the Baden-Württemberg Stiftung, the Konrad Adenauer Foundation and the Austrian Cultural Forum.

The editors, Budapest, Chișinău, Ludwigsburg and Vienna, April 2018

Welcome address by the Baden-Württemberg Stiftung

DOI: 10.24989/ocg.v331.1

After the fall of the Iron Curtain the Danube Region once again became the common cultural, economic and scientific space it used to be for centuries. However, half a century of separation and a different speed of development cannot easily be overcome. In line with the EU Strategy for the Danube Region, the Baden-Württemberg Stiftung has understood the challenge and launched its programme "Perspective Danube: Education, Culture and Civil Society". The aim of this long-term initiative is to enable sustainable cooperation in the Danube Region in order to strengthen international understanding and the creation of a robust civil society.

A modern, service-oriented Public Administration that adheres to the principles of good governance is a key factor in this endeavour. The Central and Eastern European eGovernment and eDemocracy Days are a considerable contribution that was founded in 2003 and substantially relaunched in its present form in 2014. It brings together academics and practitioners from the public sector, enabling the exchange of experience and best practices in the field. This does not necessarily mean that this exchange is one-sided: In the field of eGovernment, many administrative entities in reform countries benefit from a "late mover" advantage. They can build optimal technical and process solutions without heeding legacy systems. This can provide valuable input for others.

Furthermore, the conference provides opportunities to initiate further cooperation, such as joint project applications to H2020 and Erasmus+ thereby contributing to foster a common scientific space in the Danube Region. On the same token, we are particularly pleased to see the "Country of the Year" initiative launched with Moldova being the first Danube Region country to concisely present its legal and organisational framework for eGovernment as well as some of its most pertinent solutions. The Workshop on Smart Cities organised in cooperation with the Council of Europe will provide a further opportunity to exchange best practices in a field, which is of particularly growing importance.

On behalf of the Baden-Württemberg Stiftung, I would like to congratulate the organisers for realising this conference and the corresponding volume and I hereby wish all participants and presenters a fruitful and interesting time at CEEeGov 2018.

Dr. Andreas Weber

Head of Education Department
Baden-Württemberg Stiftung

Programme Committee

Acimovic Ivan, Stadt Freiburg im Breisgau

Awad Mohammed, American University of Ras al-Khaimah

Bagnato Domenica, Hierodiction Software GmbH

Beck Joachim, University of Public Administration Kehl

Bernhart Josef, European Academy Bozen

Cojocaru Igor, Information Society Development Institute, Chişinău

Dragomirescu Horatiu, Bucharest University of Economic Studies

Duma László, Corvinus University of Budapest

Dürrschmidt Jörg, University of Public Administration and Finance Ludwigsburg

Eixelsberger Wolfgang, Carinthia University of Applied Sciences

Fenner David, Representation of Saxony-Anhalt to the EU

Golob Blaž, GoForeSight Institute, Ljubljana

Gourova Elissaveta, Sofia University St. Kliment Ohridski

Hansen Hendrik, Andrássy University Budapest

Harsági Viktória, Andrássy University Budapest

Holzner Matthias, State Ministry Baden-Württemberg

Kiefer Andreas, Congress of Local and Regional Authorities of the Council of Europe

Kő Andrea, Corvinus University of Budapest

Kőnig Balázs, National University of Public Service, Budapest

Krasznay Csaba, National University of Public Service, Budapest

Kudo Hiroko, Chuo University

Kustor Peter, Federal Chancellery Vienna

Leiningen-Westerburg Alexander, Leiningen-Westerburg Consulting

Leitner Christine, Centre for Economics and Public Administration Ltd. (CEPA)

Lukac Irena, Center of Excellence in Finance Ljubljana

Makó Csaba, National University of Public Service, Budapest

Miloš Matija, University of Rijeka

Müller-Török Robert, University of Public Administration and Finance Ludwigsburg

Nemeslaki András, Budapest University of Technology and Economics

Nešković Siniša, University of Belgrade

Okruch Stefan, Andrássy University Budapest

Pállinger Zóltan Tibor, Andrássy University Budapest

Paulin Alois, University of Novo Mesto, Slovenija

Pautsch Arne, University of Public Administration and Finance Ludwigsburg

Pichler Johannes, Universität Graz

Pinter Róbert, Corvinus University of Budapest

Polcak Radim, Masaryk University Brno

Prosser Alexander, University of Economics and Business Administration Vienna

Rauber Andreas, Technical University of Vienna

Richter Frederick, Stiftung Datenschutz

Rihm Sebastian, Danube Office Ulm

Roggenkamp Dirk, Berlin School of Economics and Law

Rucinska Silvia, Pavol Jozef Šafárik University

Sasvári Péter, University of Miskolc

Schenk Birgit, University of Public Administration and Finance Ludwigsburg

Scola Dona, Information Society Development Institute

Setnikar-Cankar Stanka, University of Ljubljana

Setzen Florian, Europazentrum Baden-Württemberg

Sievering Oliver, University of Public Administration and Finance Ludwigsburg

Simic Diana, University of Zagreb

Szádeczky Tamás, National University of Public Service, Budapest

Traunmüller Roland, Johannes Kepler-University Linz

Urs Nicolae, Babes-Bolyai University, Cluj-Napoca

Velikanov Cyril, Memorial Society, Moscow

Vincze Attila, Andrássy University Budapest

Vrček Neven, University of Zagreb

Zait Adriana, Alexandru Ioan Cuza University of Iaşi

eGovernment I

E-CITIZENS WEB PORTAL - CASE OF CROATIA

Martina Tomičić Furjan[1], Nikolina Žajdela Hrustek[2]
and Igor Pihir[3]

DOI: 10.24989/ocg.v331.2

Abstract
Electronic government implies the use of information and communication technology (ICT) for improving the way public services are provided to all citizens. In order to create an interface, through which citizens can use these services, web portals are developed. The web portal that represents the interface for the use of services intended for citizens in the Republic of Croatia, as key users, was developed in the frame of e-citizens project, initiated by the Croatian government in year 2013. Since its inception, the portal has been continuously upgraded and complemented by new electronic services. The usage of the e-citizens portal however, despite the availability of services, does not follow the developing trends according to researches by the local Ministry of Administration and the Eurostat data. Citizens access the portal, but mostly to collect information and do not use its advanced additional functionalities. This paper analyses Croatian government web portal, its functionalities, attitudes toward it and its use by citizens. Finally, based on data analysis improvement of the accessibility/usage of Croatian government portal will be proposed.

1. Introduction

The word 'government' has several meanings, of which two are basic: a set of administrative organizations and the meaning of a particular activity [13]. To govern means to carry out joint activities in order to achieve a specific goal, through the decision-making process and implementation of these decisions.

In the initial period of creating the state, the state administration has included classic resumes such as defence, police, diplomacy, justice and finance, with the task of acting authoritatively, ignoring thereby the interests of citizens. Towards the end of the 19th century, the role of state administration was changing, encompassing activities whose primary purpose is to care for society, including education, social welfare, health, traffic, communal services, statistics, cadastre and other information services [9]. Towards the end of the eighties and early nineties of the last century, the New Public Management (NPM) is emerging, which places the citizen as a public service user in the centre of public administration. Osborne and Gaebler [12] published their work "*Reinventing government*" in 1992, which suppresses the control of public sector from being bureaucratic to society oriented.

With the growing development of information and communication technologies (ICT), the concept of electronic government emerged in the late 1990s and early 21st century. Electronic Government (e-government) is the application of information technology to the governing process with the aim of improving services for all its users [2].

[1]Faculty of Organization and Informatics, Varaždin, University of Zagreb, Croatia
[2]Faculty of Organization and Informatics, Varaždin, University of Zagreb, Croatia
[3]Faculty of Organization and Informatics, Varaždin, University of Zagreb, Croatia

The program of the Croatian government for the mandate between 2016 and 2020 [14] in one of its chapters defines modernization of the government through informatization of all public services as one of main goals. In Croatia, there are 91 services that are currently active and supported by ICT on some level of informatization [15,8]. Since these public services are results of processes, mainly performed for citizens as their consumers, on state, regional and local level, the processes themselves should be improved by use of ICT. The mentioned goal of the Croatian government is operationalized through the Strategy e-Croatia 2020 [10], which defines that e-services should be available through the e-citizen system, which is implemented through a web portal. Implementation of public e-government services should imply further use in more complex systems. One example of this use is state aid for schooling (grants, transport of students, subsidized meals etc.), that is implemented in the project *e-Schools: Establishing a System for Developing Digitally Mature Schools* [1], which is currently in progress in its pilot phase in Croatia.

2. E-citizens web portal

Web portal system called *The e-Citizens system* [8] was developed by Croatian government in year 2013, with the aim of modernization and simplification of government to citizens and citizens to government communication. Electronic services and their availability in one-point-of-contact public web portal should increase transparency and raise the quality of public service to citizens [8]. E-citizens web portal consist of three major parts that made one system for public and private use by citizens but represents one whole [8]:

1) the Central Government Portal which is the public part of the system

2) the Personal User Mailbox

3) the National Identification and Authentication System.

2.1. Central Government Portal

The central government portal represents the public part of the web portal for citizens and it's purpose is to present the structure, function and role of all state administration bodies in a single place, in a simple and modern way. The central government portal covers 12 fields of public services [15] (eg. health, employment, citizenship and personal documents…) and shares more than 485 information articles. Citizens can browse through information about available public services and be redirected to login to e-services available in the personal user mailbox, described in the next chapter.

2.2. Personal User Mailbox

The Personal User Mailbox is a private user system, protected by login credentials available to every citizen in Croatia with valid personal identification number - OIB and the appropriate credentials [17]. Citizen can access available services of their interest but also get personal messages in order to be informed about personal documents and citizens' rights for personal use like expiration of ID card, passport, driver's license or vehicle registration, polling station, rights from pension and health insurance, rights during unemployment all the way up to notification about vaccination of pets [16]. The Personal User Mailbox is available through secured web application, is also provided for smart phones Android, iPhone/iPad and Windows Phone.

2.3. National Identification and Authentication System

National Identification and Authentication System - NIAS is single point of identification and authentication of citizens' identity. Through NIAS, citizen can access e-government services listed on the central government portal and/or use them in the personal user mailbox. NIAS is a solution for identifying and authenticating users at the national level, enabling multiple types of credentials of different levels of security to be included from level 2 (lowest) to 4 (highest). This feature allows citizens to login to the e-citizen system and their personal user mailbox with already owned credential issued at other governmental systems, agencies or public content providers verified with NIAS system [8], [10], [5]. List of currently active credentials could be found at https://nias.gov.hr/Authentication/Step2; this list includes personal citizens credentials, mtoken from financial institutions, AAI educational identity credentials, credentials from several major banks used for Internet banking and other certification providers like Croatian FINA. Altogether, 16 credentials are available for use of e-services in Croatia.

According to available data from 9th November 2017, the total number of unique users with credentials is 479.848, which makes a population of all potential users that already own at least one credential supported within the NIAS system [6]. So far, access to the e-citizen system was granted to 359,979 citizens and they use it through 4,513,749 login sessions into the system [7].

3. Research data and methodology

For the purposes of further informatisation of public administration, as well as development of public e-services, The Ministry of Administration of Republic of Croatia has conducted a research on the citizens' satisfaction with electronic services and information offered by the public administration [11]. A measurement instrument (questionnaire) was developed in order to include citizens as interest parties into the creation of new public e-services and information available online. The purpose of the created measurement instrument (questionnaire) was to examine the following: which information and e-services are expected to be available on behalf of public administration, the citizens' perception connected to the quality of information and public e-services and, among others, identification of key problems and obstacles conquered by the users while using public e-services.

Measurement instrument (questionnaire) was divided into two main groups of questions. The first group consisted of questions connected to perception and usage of electronic services and information available on behalf of public administration, while the second group of questions was connected to examinees' demographic data. The group of questions connected to perception and usage of electronic services and information, consisted of 9 sub-questions used to examine the perception of examinees on the importance of access to public services and information via Internet; connected to the area of employment, judicial system, health and health services, consumers' rights, education, public data, space and environment, library catalogues, voting and citizens' participation in online public discussions and information connected to defenders and especially sensitive groups of citizens. This set of questions also consisted of questions connected to examining the citizens' satisfaction with provided information and e-services on behalf of public administration, problems and obstacles encountered during the use and possibilities of improving the e-services of public administration. For the purpose of a more complete analysis, a group of demographic questions was used in order to gather information on gender, age, level of education as well as level of informatical knowledge, profession, personal income, the availability of information and communication technologies and research participants' area and place of residence. The questions in

the measurement instrument (questionnaire) were created in form of an enclosed type with answers suggested ("Yes", "No"; "Insignificant" to "Important"; "Absolutely yes" to "Absolutely no", and additionally suggested options of answers connected to limitations, ie. obstacles in the usage of e-services) and open-type questions. The questionnaire was approached voluntarily and anonymously. The questionnaire was accessible online on the websites of the Ministry of Administration and via the e-citizen system. The period of gathering information lasted from December 17, 2014 to March 1, 2015. During the aforementioned period, over 5,100 examinees completed the questionnaire, but only 3,268 fully completed questionnaires were taken into consideration due to completeness of information taken during analysis procedures. A report was made based on the data gathered, which is accessible to the public on the websites of the Ministry of Administration of Republic of Croatia, but apart from the report on the Portal of public data [11], the original data was also published in the machine-made readable .csv form, which enabled further processing for scientific-research or business purposes to all interested users. The gathered answers served, among others, for the creation of "Draught of Strategy e-Croatia 2020".

For the purpose of this research, data and process analysis was made, and the data was taken from the previously mentioned website [11] and was elaborated via descriptive statistical analysis. The most significant results are presented in the continuation in their graphic form and are additionally descriptively explained.

4. Data analysis

An analysis of research results based on gathered/acquired data is presented in the continuation of this paper.

4.1. Demographic characteristics of respondents

Out of the total number of examinees (N=3268), 36% (N=1167) were women and 64% (N=2101) were men. Representation of all age groups was noticed. The majority of participants (33.8%, N=1105) belonged to the age group of 25-34 years of age, while the least number of participants (0.3%, N=9) were younger than 18 and older than 75. According to level of education, all suggested groups were represented as well, starting with 0.2% (N=6) with unfinished primary school and finishing with 10.5% (N=344) with postgraduate education, 52.3% (N=1708) of examinees were with undergraduate/graduate education. Connected to the level of computer literacy, the participants had to estimate which group they belonged to: "Beginner", "Average" or "Advanced" Internet users. 63.1% (N=2062) said their knowledge was "Advanced", 35.5% (N=1159) were "Average", and 1.4% (N=47) put themselves in the "Beginner" group. In relation to profession, the majority of participants (19.2%, N=626) said they worked in Natural science-technical department, 15.2% (N=496) worked in Social-humanistic area, followed by 11.8% (N=384) of "Office and counter clerks", and the least of 0.5% (N=17) were "Agricultural, hunting-breeding, forestry workers or fishermen". In relation to monthly income, 36.0% (1177) participants said they had average monthly income (3500.00-6500.00kn), while 33.6% (N=1097) received less than 3500.00kn monthly. Data on possibilities and mode of Internet access show the majority of participants (98.6%, N=3223) have the possibility of Internet access, while most of them (55.5%, N=1788) access the Internet via xDSL, and 1.4% (N=45) declared they do not want to have Internet access, due to financial or technical circumstances. According to place of residence ie. county, 37.2% (N=1212) of participants lived in Zagreb, while only 0.7% (N=27) lived in Ličko-senjska county. According to place of residence and related to the number of examinees, the majority of participants

(55.9%, N=1828) lived in localities with over 35001 inhabitants, while the least number of participants (4.9%, N=161) lived in localities with less than 500 inhabitants.

4.2. Importance of access to public services by specific areas

Data analysis established that over 96.0% of examinees said the online access to information and public services is “Considerably important“ or “Important“ when “the access to personal data on health services, health itself and making appointments for health services” is concerned. Over 91.0% of examinees are interested in “the access to judicial registers and services”, while 87.0% of examinees show interest in “the access to information and advice on consumers' rights” and “online voting”. Among all suggested areas of access to public information and services, the least number of examinees (46.6%) show interest in information on health and services connected to “Croatian defenders' rights” and “services of inclusion of especially sensitive groups” (54.7%). Considering the preferences of importance according to demographic characteristics, such as gender, three services/information present no difference in preferences to both genders. “The access to personal information on health services, health itself and making appointments for health services” and “the access to judicial registers and services” are “Considerably important” or “Important”. According to age, “the access to personal information on health services, health itself and making appointments for health services” is “Considerably important” or “Important”; the difference is the younger age groups show more interest in “online voting”, while older age groups are more interested in “the access to judicial registers and services” and “the access to information and advice on consumers' rights“.

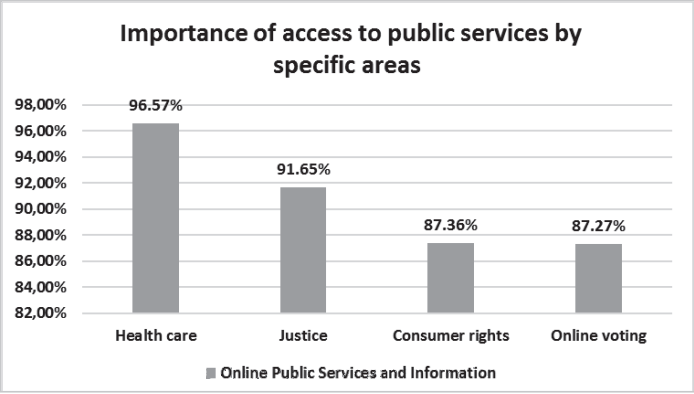

Figure 1: The importance of access to public service by specific areas

4.3. Information requested on public administration's websites within the last 12 months

Among the information the examinees searched for mostly on websites of public adminstration's bodies, one can isolate the information connected to “Personal documents” (e.g. passport, civic states, birth certificate etc.), over 84.0% (N=2754). Over 70.0% (2312) examinees searched for information on “Health and retirement insurance, social support, child's allowance”. Since the unemployment rate in Croatia is high, 49.0% of examinees searched for information on “Employment”, which is followed by 48.0% (N=1580) of searches on “Vehicles” (eg. driver's licence, registration) and 47.0% (N=1567) of searches on “Banking”. A little over 12.0% of examinees searched for the information on “Public acquisition”, and 19.0% of searches was

directed to “Information on culture and tourism”. According to gender, both groups of examinees were mostly interested in information on “Personal documents” (e.g. passport, civic states, birth certificate, etc.), while the second category with most searches was, with male population, “Health”, then “Vehicles” (e.g. driver's licence, registration). With female population, the second category with most searches was “Health and retirement insurance, social support, child's allowance”, followed by “Vehicles”. According to age groups, all age groups are equally most interested in information on “Personal documents”, “Health and retirement insurance, social support, child's allowance” and “Vehicles” (e.g. driver's licence, registration).

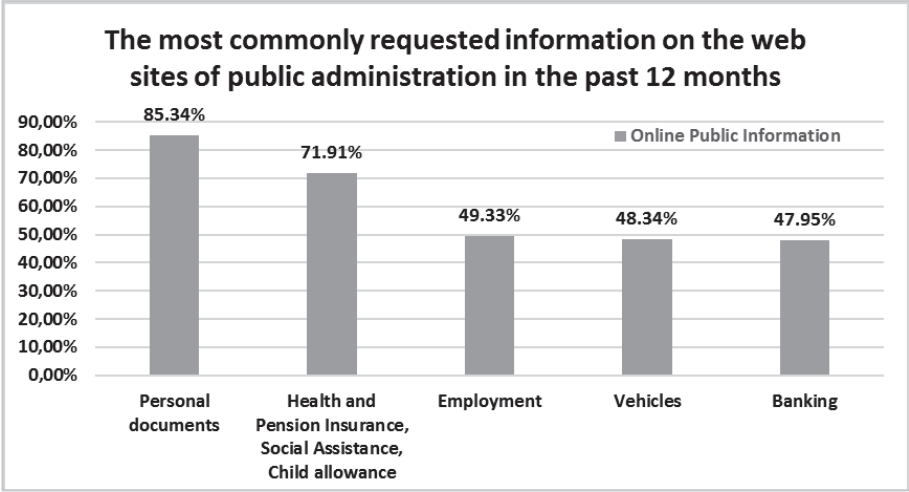

Figure 2: The most commonly requested information on the web sites of public administration in past 12 months

4.4. Experience in interacting with public administration while working on a request via its websites or online services within the last 12 months

Using websites or online services while dealing with wanted administrative requests was questioned in the manner that the examinees had to choose one out of eight claims. 36.8% (N=1204) out of the total number of examinees (N=3268) expressed a potitive attitude and said they were “satisfied with the way the body of authority solved their question”. Among the presented flaws connected to the electronic business of public administration, over 21.0% (N=685) examinees said “dealing with the wanted administrative request is impossible via the Internet”, 10.6% (N=346) said “the procedure of handing in and processing the requests is complicated and instructions are difficult to understand”, and little less than 10.3% (N=335) declared “the processing of their administrative question took longer than expected”. 7.9% (N=259) examinees said they “have not received neither the answer nor a response from the body of authority”, 3.3% (N=107) said “the form was too difficult and instructions were missing or were not understandable”, and 2.8% (N=92) came across “technical problems” while using the website or public administration's online service. Taken from the perspective of changes introduced by public administration and connected to websites and online services, 40.9% (N=1336) of examinees said they noticed the said changes and no less than 78.0% (N= 1042) considered them “positive”.

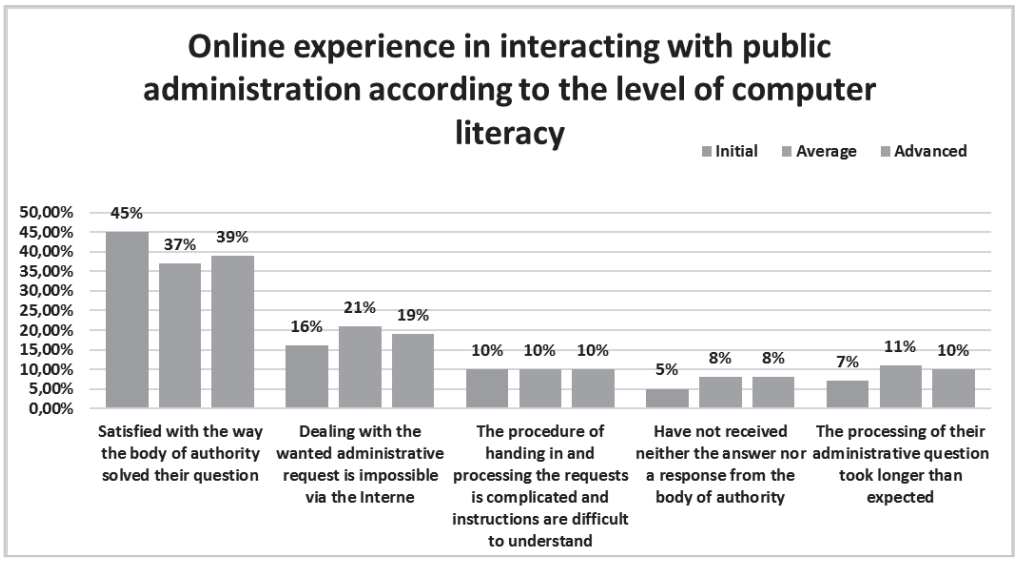

Figure 3: Online experience in interacting with public administration according to the level of computer literacy

4.5. Examinees' interest in using online public bodies' services

When asked about the interest in using online public bodies' services, the answers provided by examinees clearly show that the interest is very high. 98.8% or (N=3229, with total N=3268) declared themselves with “Absolutely yes” or “Probably yes”, while only 0.5% (N=15) said they “would not” use the said services, ie. 0.7% (N=24) said they “do not know” how to use them. The analysis according to age groups shows that the greatest interest in using online public bodies' services among the examinees is in groups 25-34 and 35-44 years of age.

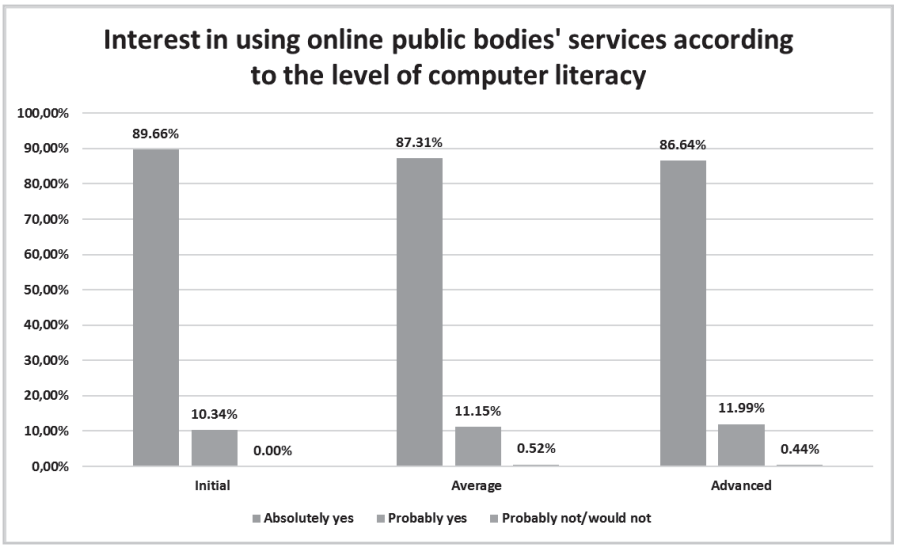

Figure 4: Interest in using online public bodies' services according to the level of computer literacy

4.6. Limitations in using online services

The continuation of this paper will present the most important limitations the examinees consider to be key limitations while using online public administration services. "The small number of available services" was isolated as the most important limitation (24.9%; N=2082), which is followed by limitation connected to dealing with further procedures after the completion of online forms due to the inability of using the e-signature. "In the end, I still have to go to the authorised office in order to personally sign or collect the wanted document" (19.6%; N=1634). 18.7% (N=1565) of participants said there is "a lack of services the citizens are interested in", while a little over 10.2% (N=855) said there is "a lack of information on how to operate". As the fifth most important limitation (10.0%; N=835), the citizens' mistrust and concerns connected to online services are mentioned, ie. "the insecurity whether requests will eventually be handled with properly". 2.4% (N=198) of examinees agreed with the claim that "the security is not on a required level", when the issue of privacy and personal data protection is mentioned. It is interesting to emphasise that only 7.0% of examinees said there are "no limitations for them" while using online public services, while only 1% (N=85) declared they have "bad experience" while using public online services.

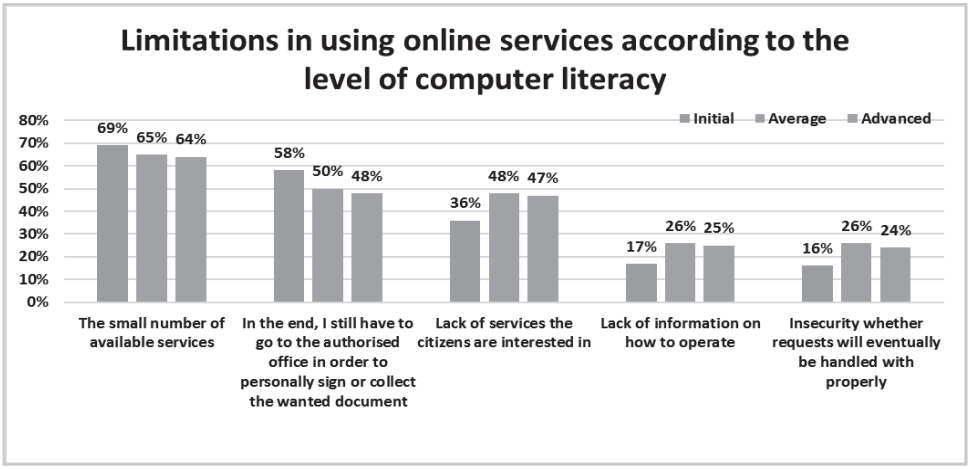

Figure 5: Limitations in using online services according to the level of computer literacy

4.7. Data analysis - The most important services and information on the public sector which need to be accessible online

In this part of the measurement instrument (questionnaire), the research participants had to make a decision on three most important areas, which should be provided online by the public administration. The majority of examinees, over 20.0%, agreed this should be the information and services connected to "Finances and taxes", while the second most important area of their choice, for over 16.0% of examinees, was "Health". Over 10.0% of examinees are interested in services and information connected to "Legal state and security", over 9.0% are interested in "Upbringing and education", and over 8.0% want to know more about "Employment". The least number of examinees, less than 0.7%, declared themselves as having interest in information and services connected to "Culture", while less than 1.1% out of the total number of examinees want to know more about "Tourism".

5. Discussion and Recommendations for improvement

European statistics show that citizens of Croatia interact with the state administration using e-government services in 32% of cases while the EU 28 average for 2017 is 49%. Most advance EU member state is Denmark with 89% [4]. When viewed from the perspective that Croatia joined the European Union as a last member state in year 2013, these results should be considered as good in relation to other comparable EU countries (like Bulgaria, Romania, Poland etc). From the point of availability and level of informatisation of e-services, their quantity and quality, through the analysis in this paper, few limitations of current e-government system were identified, and as a conclusion of this paper, there are some recommendations that can be used for improvement of the identified limitations:

1) **The small number of available services** – from the citizen's perspective the number of online services is limited, and they need to choose what to do "online" and what "manually" in government offices. Our recommendation is to make more services electronic, in accordance with the goal mentioned in the introduction of this paper and defined in the Strategy e-Croatia 2020 [10].

2) **Dealing with further procedures after the completion of online forms due to the inability of using the e-signature** –some services can be started or initiated "online" but citizen still need to do "manual" steps in order to finish the service in government offices. This happens due to the lack of electronic identity and personal certificate and/or its corresponding security level for every citizen. Without appropriate credentials, some services are not electronically covered from-start-to-finish, and that prevents government bodies and agencies to create complete electronic services. Recommendation is to make services completely electronic (from request to the end of service) and that means to build necessary infrastructural, legal and practical environment for that. Multiple use of e-identity (personal certificate of citizens, commonly on every identity card in developed countries) in real life processes would be cost effective. Recommendation is also to do a systematic analysis of all services ("e-services" and "manual services") from process perspective, by using the *Process life cycle* described in Dumas et al [3] and systematically build the environment for complete e-government. Best practice and known solutions from other leading countries in the field of e-government should as well be used for implementation of this recommendation.

3) **A lack of services the citizens are interested in** – Recommendation is to give the opportunity to citizens to say what they consider important and then to use scientific research analysis and results as a baseline to decide what services are more important and more useful to citizens. Some areas of governmental services are already described and ranked by citizens' perspective of what is important to be available as an e-service in the analysis in this paper (see chapter 4.7.) and this can be further researched.

4) **A lack of information on how to operate** – from the citizens perspective, some e-service delivery ways are “to complicated”, or just too “new”, and they feel more secure and confident doing them "manually", rather than first learn how to do them online and then really try doing them online. Recommendation is to create: guidelines for every e-service, video instructions, build e-service applications as an expert system that helps users to define what they need and help them go through the whole e-service process step-by-step. So called "smart systems or virtual assistant systems" could be used to guide citizens through the whole e-service. Also,

emphasis on the benefits of every e-service (time and cost savings), would give citizens more motivation to use them in the electronic way.

5) **The insecurity whether requests will eventually be handled with properly** – citizens feel unsafe in an online environment, they don't trust new technology or have insufficient computer skills to comformly use e-services instead of manual services. Recommendation is to work more in general on raising citizens' awareness of the role of public administration, on increasing public trust in the government and the public institutions and the processes that are being run and implemented there.

6. References

[1] CARNet, e-Schools: Establishing a System for Developing Digitally Mature Schools (pilot project) – Project description, Accessed 1st December 2017 from www.e-skole.hr/en/e-schools/project-description/ .

[2] CHEN, H., BRANDT, L., GREGG, V., TRAUNMUELLER, R., DAWES, S., HOVY, E., MACINTOSH, A. and LARSON, C. A., Digital Government, E-government Research, Case Studies, and Implementation. Springer, New York, USA 2008.

[3] DUMAS, M., LA ROSA, M., MENDLING, J. and REIJERS, H. A., Fundamentals of Business Process Management, Springer Verlag, Berlin 2013.

[4] Eurostat, Individuals using the internet for interaction with public authorities, Accessed 1st December 2017 from http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00012&plugin=1

[5] FINA, ePASS, FINA, 2017, Accessed 1st December 2017 from https://epass.gov.hr .

[6] gov.hr a, C_KorisniciSustavaEgradani – Ukupni broj jedinstvenih korisnika. Accessed 1st December 2017 from https://gov.hr/UserDocsImages//Data%20za%20datagov.hr/MURHeGradjaniStat//C_KorisniciSustavaEgradani.xml

[7] gov.hr b. D Koristenje usluga, Accessed 1st December 2017 from https://gov.hr/UserDocs Images//Data%20za%20datagov.hr/MURHeGradjaniStat//D_Koristenje_usluga.xml .

[8] Government of the Republic of Croatia, The e-Citizens system, 2017, Accessed 1st December 2017 from https://vlada.gov.hr/the-e-citizens-system/15215 .

[9] KOPRIĆ, I., Javna uprava – nastavni materijali, ur. Koprić, I., Suvremena javna uprava, Zagreb 2006.

[10] Ministarstvo uprave a, Strategija e-Hrvatska 2020, Ministarstvo uprave RH, Hrvatska, 2017.

[11] Ministarstvo uprave b. Zadovoljstvo građana elektroničkim uslugama i informacijama u javnoj upravi podaci istraživanja. Ministarstvo uprave, 2015, Accessed 1st December 2017 from http://data.gov.hr/dataset/zadovoljstvo-gradjana-elektronickim-uslugama-i-informacijama-u-javnoj-upravi

[12] OSBORNE, D. and GAEBLER, T., Reinventing government, Addison-Wesley Publ. Co., USA 1992.

[13] PUSIĆ, E., Nauka o upravi, Školska knjiga, Zagreb 2002.

[14] Vlada RH a, Program Vlade Republike Hrvatske za mandat 2016-2020. Vlada RH, Hrvatska, 2016.

[15] Vlada RH b, Središnji državni portal – Moja uprava, Vlada RH, Hrvatska, 2017, Accessed 1st February 2018 from www.gov.hr/moja-uprava/22

[16] Vlada RH c, O središnjem državnom portalu, Vlada RH, Hrvatska, 2017, Accessed 1st December 2017 from www.vlada.gov.hr/sredisnji-drzavni-portal/203 .

[17] Vlada RH d, Osobni korisnički pretinac, Vlada RH, Hrvatska, 2014, Accessed 1st December 2017 from https://pretinac.gov.hr/KorisnickiPretinac/eGradani.html

EGOVERNMENT AS AN ELEMENT OF THE RIGHT TO GOOD ADMINISTRATION

Justyna Matusiak[1] and Marcin Princ[2]

DOI: 10.24989/ocg.v331.3

Abstract

The right to good administration constitutes an established principle of European Union law, which includes the procedural rights of stakeholders in administrative proceedings, the result of which may affect their interests. Article 41 of the European Union Charter of Fundamental Rights states that every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions and bodies of the Union. When it comes to reasonable time of handling the case one can ask if eGovernment solutions are the guarantee of such a right.

eGovernment understood as the use of all kinds of electronic means of communication, in particular, however, the Internet, improves services provided by the state to its citizens. The usage of IT technology in public administration allows it to perform its activities in a more efficient way. This improvement applies not only to the communication between parties but also to the quality of citizens' life.

To sum up, one can ask the question if the European right to good administration can be understood as the right to eGovernment solutions and if so, to what extent. Which services and technical solutions should be guaranteed as ones ensuring challenges of good administration?

1. Introduction

The right to good administration, as well as eGovernment are two separate challenges facing current public administration. This means that, on one hand, administration must meet current standards of, so called, good administration, and on the other, it must meet contemporary requirements of the information society.

The purpose of this paper is to answer the question whether there is any relationship between the above topics. The research problem of this study comprises mainly issues of European administrative law. The study presents fundamental themes of defining the right to good administration and the concept of eGovernment. Furthermore, the study shows examples of the implementation of law for good administration, with special attention to eGovernment solutions.

The implementation of the aforementioned law requires financial spending from the central-government budget. Current public administration that meets ICT standards is not cheap. The struggle for funds from central-government budget is increasing in intensity, since there is a steady increase of spending at the level of social, health, and educational requirements. How to justify

[1] WSB University in Poznań, Institute of Law and Administration, Powstańców Wielkopolskich 5, 61-895 Poznań, Poland, justyna.matusiak@wsb.poznan.pl, http://www.wsb.pl/english/.
[2]Adam Mickiewicz University in Poznań, Faculty of Law and Administration, al. Niepodległości 53, 61-714 Poznań, Poland, m.princ@amu.edu.pl, https://prawo.amu.edu.pl/en.

additional expenditure on eAdministration? One justification may be the fact that eGovernment is an element of the right to good administration.

2. Defining the right to good administration

The 20th century brought about a number of changes in the perception of existing relations and institutions. One good example in that respect is the legal construction of citizenship, which changed the relationship between the state and the individual. Citizens, apart from the obligations imposed on them, gained a lot of rights under the agreement which ties them to the state.

The establishment of right to good administration is the result of the development of society. This is also stressed by I. Lipowicz [1], the Ombudsman in Poland in the years 2010-2015, who states, that the existence of the right to good administration comes from an increased citizenship awareness. It is appropriate to support the claim that the administered no longer wanted to sit back and merely watch what is happening in public administration, but rather want to have their say in pursuing the ideal [2].

The subject of good administration resurfaced with the creation of the Charter of Fundamental Rights of the European Union [3] and the European Code of Good Administrative Behavior. The right to good administration is set out in Article 41 of the Charter. It stipulates that "Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the Union. Additionally, the Charter guarantees "the right of every person to be heard, before any individual measure which would affect him or her adversely is taken", "the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy" and "the obligation of the administration to give reasons for its decisions". In addition, it is stipulated that: "Every person has the right to have the Union make good any damage caused by its institutions or by its servants in the performance of their duties, in accordance with the general principles common to the laws of the Member States" and that: "Every person may write to the institutions of the Union in one of the languages of the Treaties and must have an answer in the same language*"*.

It should be stressed that the provisions of the Charter were incorporated in the Treaty provisions. Within the meaning of Article 6.1 of the Treaty of Lisbon amending the Treaty of the European Union and the Treaty Establishing the European Community [4] and signed in Lisbon on 13 December 2007, the Union recognizes the rights, freedoms, and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, in the wording finalized on 12 December 2007 in Strasbourg.

The wording of Article 41 of the Charter is a compromise of sorts. The current understanding of the requirements of good administration is undoubtedly also under the influence of the provisions of the European Code of Good Administrative Behavior (European Code of Good Administrative Practice), recommendation R (2007) 7 of the Committee of Ministers of Member States concerning good administration, or the drafted European Union Code of Conduct [5, 6, 7]. Among the provisions set out in the aforementioned legal acts there are, inter alia, the following rules which are part of the current understanding of good administration: rule of law, equality, impartiality, proportionality, legal certainty, undertaking actions at the right time, participation, respect for privacy, principle of coherence and reasonable expectations, transparency, principle of efficiency and utility, and the principle of honesty.

The right to good administration is interpreted in different ways. According to Z. Cieślak [8], it can be understood as:

1) the right of a citizen, who by interacting with administration, is entitled to demand that the right to good administration be exercised,

2) public subjective right shaped by legal procedures and institutions which are to implement the demand for exercising good administration,

3) pseudo-legal category – understood as a non-binding legal rule resulting from and summarizing the legal system,

4) non-legal category – understood as a social phenomenon deriving from political relations, social aspects, based on ethical assessments.

Presently, one should fully agree with I. Lipowicz's [9] opinion, that the adoption of the Charter of Fundamental Rights of the European Union transferred the right of good administration from the non- and pseudo-legal categories to the set of "civil rights" of EU citizens. This right is usually defined as a set of procedural subjective rights [10, 11], sometimes, with its individual elements, classified within the framework of procedural dignity [12]. Following the European legislator who placed it in the fundamental legal act, i.e. in the Charter of Fundamental Rights of the EU, we should suppose that we are dealing with a fundamental right [13], which still has an unclear status of an "umbrella-right" [14]. At the same time, it should be noted that some legal theorists place the right to good administration in the category of, so called, third generation rights [15]. Sometimes, however, it is claimed that this right cannot be considered in the category of human rights stemming from the innate and nontransferable dignity of the human being, but rather they should be associated with the construction of a democratic rule of law [16].

The right to good administration is a European standard [17]. At the same time, equally valid is the opinion expressed by W. Chróścielewski and Z. Kmieciak [18], who claim that the right to good administration at present can be associated with a set of legal standards referring to public administration activities so cohesive, unambiguous and precise that they can be treated as evaluation criteria for assessing the correctness of different solutions existing within the national legal order. In the implementation of standards the national legislator is free to select the means of such implementation [19].

It seems safe to say, that on the basis of the classic three-branch separation of powers, with respect to the legislative power of the highest importance are the principles of decent legislation, with respect to the judicial power – the principle of fair procedure and the right to a fair trial, consequently, with respect to the executive power, public administration in particular, the right to and principle of good administration.

3. eGovernment – computerization of public entities

The legal basis for the existence of good practices in administrative bodies can be derived from different regulations related to administrative law, including also in areas where the process of computerization of public authorities is prominently visible [20].

The definition of eGovernment evolved over time, and in literature one can find different approaches to its definition, as analyzed, e.g. by R. Gil-Garcia [21]. For the purposes of this study one can adopt the definition proposed by the Author who points that electronic government is a selection, design, implementation, and use of information and communication technologies in government to provide public services, improve managerial effectiveness, and promote democratic values and participation mechanisms, as well as the development of a legal and regulatory framework that facilities information intensive initiatives and fosters the knowledge society. In other words, eGovernment refers to the use of information and communication technology tools and applications to enhance government transparency and accountability in public administration by improving public services delivery, access to information and services and public governance [22]. Public governance, which is a concept which can be understood more broadly than eGovernment, is a process of managing a complex society with the participation of entities from the public and private sectors, often in the form of a network, in which the central place does not have to belong to public administrative authorities [23].

The element which appears in most eGovernment-related definitions is effectiveness (consequently, also a resolution of a matter within a reasonable time), and democratic principles (specifically, impartiality and fairness). In literature [24, 25] there are many studies which point whether and how these goals have been achieved. S. Bhatnagar [26] gives specific examples of saving time after the introduction of eGovernment solutions in such places as Brazil, Chile, China, India, Jamaica, the Philippines, or Singapore. Although the implementation of eGovernment related projects still faces many problems, in many countries, including Poland, the Czech Republic, or Germany, the question is being asked whether it counts from the point of view of good administration. It has to be underlined that failures, which vary from not establishing project success to missing citizen expectations and adoption, even to preferences in turning back to traditional channel section (i.e. face-to-face visits and voice phone calls) cause the questioning of both eGovernment feasibility and sustainability [27].

Electronic government (eGovernment) comprises electronic administration (eAdministration), i.e. electronic services provided to natural persons and businesses provided by public entities, and electronic democracy (eDemocracy), i.e. citizens' active participation in political life to improve their quality of life. eAdministration, which uses modern tools provided by information and communication technologies, is often pointed to as the key initiator and performer of the changes which are taking place [28]. Thanks to some unchanging attributes, public administration can use IT techniques in such a way, so as to perform its activities in the most efficient manner.

eAdministration is not the contradiction of the ideal bureaucratic structure formulated by Max Weber. Although eAdministration is described [29] as non-bureaucratic, transparent, effective, cheap, and fast, i.e. efficient and friendly, this is not exactly the truth. The handling of cases in a bureaucratic way simply means that they are managed in accordance with the rules of a bureaucratic organization, which organization is the materialization of the concept of the rule of law. Consequently, one can postulate [30] that attempts are being made to reform the bureaucratic organization of public administration, and use new technologies to implement this reform. Literature states [31] that the Weberian model is such a form of organization which in the nearest future, at least over the next few decades, will still be in place. If a new type of the organizational form is to appear, then it is hard to specify how it will look like. Therefore, it is said, that presently one can only talk about bureaucracy being under the influence of information technologies, about information-based bureaucracy. Such position expressed in literature [32], is connected with another concept, namely eBureaucracy. Authors state that eBureaucracies are organizations that

follow the procedural logic of a public bureaucracy, to coordinate the execution of organization activities, and hence to deliver services, but rely on ICTs to sustain procedural efficiency. ICTs are used in order to facilitate and support the fundamental organizational functions of coordination and control of bureaucratic organizations. These functions are defined in the legal-normative set of rules designed to standardize the administrative procedure and the delivery of public services. As mentioned in literature [33] eGovernment can be seen as the application of information and communication technologies in order to redesign ways in which governments exchange information with stakeholders but ICTs do not transform government by themselves. State structures, pre-existing institutional structures, legal, regulatory and cultural factors determine how specific technological innovations look and how specific institutional change will take place.

When it comes to solving eGovernment problems the meaning of comparative legal research has to be underlined. To ensure success of eGovernment, more research is required to determine which exact solutions can be defined as guarantees of the right to good administration. As mentioned by V. Homburg [34], one way of exploring specific relations between characteristics of technology on the one hand and institutional, social, economic and political factors on the other hand, is to scrutinize and compare technologies in various settings, for example countries. Such studies could inform of what exact constellations of actors, interests, power bases and control potentials stimulate, mediate or obstruct technology in public administration. eGovernment is based on national and local sets of rules. The need exists for each country to understand and improve the effective and efficient use of eGovernment for information exchange at an international level [35]. J. T. Snead and E. Wright underline that more theory-based efforts are needed to understand eGovernment as a field of study.

4. Relationship between eGovernment and right to good administration

It is worth emphasizing that good administration standards, understood as a theoretical generalization of both principles and guidelines, are connected with good governance requirements [36, 37, 38, 39, 40], or in general with the notion of democratic rule [41]. In particular, direct relationship occurs with such principles as: co-participation on equal rights, rule of law, transparency, punctuality, partnership and social dialogue (the consensus principle), fairness and share, efficiency and productivity, as well as responsibility [42]. Presently, good administration standards together with other constitutional norms restrict reforms undertaken in the country [43].

By way of illustration, in Poland the right to good administration has not been directly expressed in the national legal system. However, the good administration principle can be recognized as a legal principle stemming from the notion of the democratic rule of law, and also corresponding with other constitutional norms [44]. A similar situation is in other European countries, e.g. in Romania [45]. Right to good administration and principle of good administration have also been used in legal practice, e.g. regarding changes in the land and building register [46], in case of mutual information and cooperation between institutions [47], in the matter of occupying the road lane [48], in the scope of excessive length of proceedings regarding the tax on goods and services [49], regarding inactivity in the field of property expropriation [50].

Some Authors notice [51], that the right to good administration can be understood in a broader way and cover not only eGovernment but also eGovernance. That is because, as already mentioned, the right to good administration comprises in itself the right to good governance. In such understanding, the key elements of good governance comprise effective mechanisms for citizen participation, a transparent and corruption-free political system, accountability of public authorities, modern

administrative services, inclusion of vulnerable groups and introduction of eGovernance. The transformation from eGovernment to eGovernance comes from the rise of eParticipation and is much more than just providing information and services. It is the usage of information and communication technologies at various levels of the public sector and beyond for the purpose of enhancing governance [52].

The core of the right to good administration resulting from the Charter of Fundamental Rights of the EU is for all affairs to be handled impartially, fairly and within a reasonable time. This condition can be met by using eGovernment solutions, e.g. by eliminating the human element and human's discretionary nature. Often, eGovernment solutions are perceived as tools to fight corruption or eliminate arbitrariness of decisions taken by public administration. In addition, reliability of administrative proceedings can be guaranteed by eGovernment solutions by way of ensuring that every procedure is clearly defined, and will follow strict principles, e.g. on the basis of the principle of providing information using continuous and current access to information and events taking place during administrative proceedings (e.g. access websites like www.borger.dk in Denmark). eGovernment can be considered from the point of view of time savings, but also knowledge about the starting time and closing time of administrative proceedings. Thanks to ICT solutions both the party involved and the supervisory authority can have information about the excessive length of the proceedings and inactivity of the administrative body.

Thus the question arises, whether all eGovernment solutions guarantee the right to good administration. In addition, whether this applies only to services characteristic for eAdministration, or more broadly, also services related to eDemocracy, eParticipation, or eVoting.

The authors of this paper hold the position that all properly interpreted eGovernment solutions guarantee the right to good administration. In their opinion, this applies not only to solutions characteristic for eAdministration, but also e.g. eDemocracy. The right to good administration does not merely apply to the affairs of an individual, with respect to public administration, handled by way of a decision, order or administrative arrangement [53], but in a broader meaning, it may also apply to different contacts between entities being subject to administration, with the administrative bodies themselves, which consists of different forms like questions, requests, protests, filing comments to draft legal regulations, or bills initiated by citizens. One must however underline that it is impossible to illustrate the link between the right to good administration and eGovernment issues on factual lawsuits or legal practice.

The aforementioned legal and comparative studies gain paramount importance from the point of view of the right to good administration. Legal and comparative studies should be continued in that respect, while an attempt to answer the question about relations between the right to good administration and eGovernment is becoming an important one in the context of administrative law.

5. Summary

Summarizing the above considerations, it should be pointed that although the issues of the right to good administration and eGovernment may seemingly be not connected, in fact the relationship between them is quite strong. This analysis shows that implementation of eGovernment projects may be financially justified in the light of the principles of good administration. Additionally, such projects fulfill the right to good administration. The three key pillars, namely impartiality, fairness and reasonable time of resolving affairs can be achieved in fact by eGovernment projects. Additionally, this applies not only to the narrowly understood eAdministration, but broadly

considered eGovernment, and even eGovernanace or good governance. While there is a high number of studies and analyses focusing on each of these concepts separately, it is very rare, if at all, to find a study that would identify eGovernment as a guarantor of implementing the principle of good administration. Without any question, good administration requirements were connected with the concept of good governance.

The scope of this paper allowed the Authors to only highlight the fundamental issues related to the definition of the aforementioned concepts or methods of implementation, but at the same time allowed them to clearly express the conviction that they concepts interpenetrate one another. Furthermore, it should be reiterated that studies in this area should be continued and broadened, in particular legal-and-comparative studies, taking into account existing and planned solutions related to the right of good administration, eGovernment at European level, and at national levels in member state legal systems.

6. References

[1] LIPOWICZ, I., Prawo obywatela do dobrej administracji [A citizen's right to good administration], in: Hauser, R., Nowacki, J. (ed.), Państwo w służbie obywateli. Księga jubileuszowa Jerzego Świątkiewicza [The state in the service of citizens. Jerzy Świątkiewicz's jubilee book], Łódź: "Master", Warsaw 2005, p. 130.

[2] SZPOR, A., Odwaga służenia dobru wspólnemu [Courage to serve the common good], in: Niewiadomski, Z., Cieślak, Z. (ed.), Prawo do dobrej administracji, Materiały ze Zjazdu Katedr Prawa i Postępowania Administracyjnego, Warszawa – Dębe 23-25 września 2002 [Right to good administration. Materials from the convent of Law and Administration Procedure Faculties Warszawa-Dębe 23-25 September 2002], Wydawnictwo Uniwersytetu Kardynała Stanisława Wyszyńskiego, Warsaw 2003, p. 640.

[3] The Charter of Fundamental Rights of the European Union proclaimed in Strasbourg on 12 December 2007 by the European Parliament, Council and Committee (Official Journal C 303 of 14 Dec. 2007, p. 1).

[4] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community signed in Lisbon on 13 December 2007 (EU Journal of Laws C 306 of 2007, p. 1).

[5] European Parliament resolution of 15 January 2013 with recommendations to the Commission on a Law of Administrative Procedure of the European Union, P7_TA(2013)0004, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0004+0+DOC+XML+V0//PL (10 Oct. 2013).

[6] SUPERNAT, J., Dobra administracja w prawie Unii Europejskiej [Good administration in European Union law], in: Sługocki, J. (ed.), Dziesięć lat polskich doświadczeń w Unii Europejskiej. Problemy prawnoadministracyjne [Ten years of Polish experiences in European Union. Legal and administrative problems], v. 1, PRESSCOM Sp. z o.o., Wrocław 2014, pp. 665-667.

[7] PRINC, M., Komentarz do Rezolucji Parlamentu Europejskiego z dnia 15 stycznia 2013 r. zawierającej zalecenia dla Komisji w sprawie prawodawstwa dotyczącego postępowania

administracyjnego w Unii Europejskiej [Comments to the European Parliament resolution of 15 January 2013 with recommendations to the Commission on a Law of Administrative Procedure in the European Union], Studies in Public Law 4 (2013), pp. 175-188.

[8] CIEŚLAK, Z., Prawo do dobrej administracji (tezy wystąpienia) [Right to good administration (topics of the speech)], in: Niewiadomski, Z., Cieślak, Z. (ed.), Prawo do dobrej administracji, Materiały ze Zjazdu Katedr Prawa i Postępowania Administracyjnego, Warszawa – Dębe 23-25 września 2002 [Right to good administration. Materials from the convent of Law and Administration Procedure Faculties Warszawa-Dębe 23-25 September 2002], Wydawnictwo Uniwersytetu Kardynała Stanisława Wyszyńskiego, Warsaw 2003, p. 18.

[9] LIPOWICZ, I., O mądre prawo i wrażliwe państwo [For a wise law and sensitive country], Biuletyn Rzecznika Praw Obywatelskich 80 (2013), p. 67.

[10] BRODECKI, Z., Substrat – prawo [Substrate – the law] [in:] BRODECKI Z. (ed.), Europa urzędników [A Europe of officials], LexisNexis Polska, Warsaw 2009, p. 76.

[11] KMIECIAK, Z., Postępowanie administracyjne i sądowo administracyjne a prawo europejskie [Administrative and court-and-administrative procedure vs. European law], Wolters Kluwer Polska, Warsaw 2010, p. 60.

[12] BRODECKI, Z. (ed.), Europa urzędników [A Europe of officials], LexisNexis Polska, Warsaw 2009, p. 99.

[13] SZYDŁO, M., Prawo do dobrej administracji jako prawo podstawowe w unijnym porządku prawnym [The right to good administration as a fundamental right in EU legal system], Studia Europejskie 1 (2004), p. 87-107.

[14] MENDES, J., Good administration in EU Law and European Code of Good Administrative Behaviour, EUI Working Paper 9 (2009), p. 4.

[15] LIPOWICZ, I., O mądre prawo i wrażliwe państwo [For a wise law and sensitive country], Biuletyn Rzecznika Praw Obywatelskich 80 (2013), p. 65.

[16] DOBKOWSKI, J., Kodeks dobrej administracji Rady Europy (geneza – charakter – treści) [Code of good administration of the Council of Europe (origin – character – content)], in: Niczyporuk, J., Kodyfikacja postępowania administracyjnego na 50 lecie K.P.A. [Codification of the administrative procedure on the occasion of the 50th anniversary of the Code of Administrative Procedure],Wydawnictwo WSPA, Lublin 2010, p. 138.

[17] JACKIEWICZ, A. I., Prawo do dobrej administracji jako standard europejski [The right to good administration as a European standard], Wydawnictwo Adam Marszałek, Toruń 2008.

[18] CHRÓŚCIELEWSKI, W., KMIECIAK, Z., Kodeks postępowania administracyjnego a prawo do dobrej administracji [Code of administrative procedure and the right to good administration], in: Niczyporuk, J., Kodyfikacja postępowania administracyjnego na 50 lecie K.P.A. [Codification of the administrative procedure on the occasion of the 50th anniversary of the Code of Administrative Procedure], Wydawnictwo WSPA, Lublin 2010, p. 68.

[19] PRINC, M., Standardy dobrej administracji w prawie administracyjnym [Standards of good administration in administrative law], Wydawnictwo UAM, Poznań 2017, p. 113-114.

[20] TOMASZEWSKA, K., Dobre praktyki organów administracji publicznej w dostępie do geoinformacji w świetle ustawy o infrastrukturze informacji przestrzennej [Good practice of public administrative authorities in the access to geoinformation in the light of the Act on Infrastructure of Spatial Information], in: Gołaczyński, J. (ed.), Wybrane dobre praktyki w zakresie usług elektronicznych [Selected good practice regarding electronic services], C. H. Beck, Warsaw 2016, pp. 115-116.

[21] RAMON GIL-GARCIA, J., Enacting Electronic Government Success. An Integrative Study of Government-wide Websites, Organizational Capabilities, and Institutions, Springer, New York 2012, pp. 4-17.

[22] AL-HUJRAN, O., AL-DEBEI, M. M., CHATFIELD, A., MIGDADI, M., The imperative of influencing citizen attitude toward e-government adoption and use, Computers in Human Behavior 53 (2015), pp. 189-203.

[23] SUPERNAT, J., Administracja publiczna, governance i nowe publiczne zarządzanie [Public administration, governance and new public management], in: Blicharz, J., Boć, J. (ed.), Prawna działalność instytucji społeczeństwa obywatelskiego [Legal activity of civil society institutions], Kolonia Limited, Wrocław 2009, p. 139.

[24] FUGINI, M. G., MAGGIOLINI, P., VALLES, R. S., e-Government and Employment Services. A Case Study in Effectiveness, Springer, Cham 2014.

[25] RODRIGUEZ-BOLIVAR, M., P. (ed.), Measuring E-government Efficiency. The Opinions of Public Administrators and Other Stakeholders, Springer, New York 2014.

[26] BHATNAGAR, S., Unlocking E-Government Potential. Concepts, Cases and Practical Insights, SAGE Publications, New Delhi 2009, p. 32.

[27] ANTHOPOULOS, L., REDDICK, Ch. G., GIANNAKIDOU, I., MAVRIDIS, N., Why e-government projects fail? An analysis of the Healthcare.gov website, Government Information Quarterly 33 (2016), pp. 161-173.

[28] DR PERRI 6, E-governance. Styles of Political Judgement in the Information Age Polity,Palgrave Macmillian, New York 2004, p. 16.

[29] DĄBROWSKA, A., JANOŚ-KRESŁO, M., WÓDKOWSKI, A., E-services and the information society [E - usługi a społeczeństwo informacyjne], Difin, Warsaw 2009, p. 48.

[30] HOMBURG, V., Understanding E-government: Information systems in public administration, Routledge, New York 2008, p. 57.

[31] FOUNTAIN, J. E., Toward a Theory of Federal Bureaucracy for the Twenty-First Century, in: Kamarck, E. C., Nye Jr., J. S. (ed.), Governance.com. Democracy in the Information Age, Booking Institutions Press, Washington 2002, pp. 118-119.

[32] CORDELLA, A., TEMPINI, N., E-government and organizational change: Reappraising the role of ICT and bureaucracy in public service delivery, Government Information Quarterly 32 (2015), pp. 279-286.

[33] POLLITT, Ch., VAN THIEL, S., HOMBURG, V., New Public Management in Europe, Management Online Review, 10 (2007), pp. 1-7.

[34] HOMBURG, V., Understanding E-government: Information systems in public administration, Routledge, New York 2008, pp. 126-127.

[35] SNEAD, J. T., WRIGHT, E., E-government research in the United States, Government Information Quarterly 31 (2014), pp. 129-136.

[36] KRAWIEC,G., Europejskie prawo administracyjne [European administrative law], Wolters Kluwer Polska, Warsaw 2009, pp. 23-25.

[37] WAKEFIELD, J., The right to good administration, Kluwer Law International, The Hague 2007.

[38] STEFAŃSKA, E., Decyzje o odmowie przyznania własności czasowej nieruchomości w trybie dekretu warszawskiego jako przykład patologii w funkcjonowaniu administracji [Decisions on refusal to grant temporary ownership to real property under the Warsaw decree as an example of pathology in the operation of administration], in: Suwaj, P. J., Kijowski, D. R., Patologie w administracji publicznej [Pathologies in public administration], Wolters Kluwer Polska, Warsaw 2009, p. 356.

[39] IZDEBSKI, H., Zasada dobrej administracji i prawo do dobrej administracji w świetle standardów Rady Europy [The principle to good administration and the right to good administration in the light of the standards of the Council of Europe], in: Machieńska,H., 60 lat Rady Europy. Tworzenie i stosowanie standardów prawnych [60 years of the Council of Europe. Creation and application of legal standards], Wydawnictwo Wiedza i Praktyka, Warsaw 2009, p. 324.

[40] IZDEBSKI, H., Fundamenty współczesnych państw [Foundations of current states], Wydawnictwo Prawnicze LexisNexis, Warsaw 2007, p. 210 ff.

[41] OBAIDULLAH, A. T. M, Democracy and good governance. The role of ombudsman, Bangladesh Institute of Parliamentary Studies, Dhaka 2001, p. 1 ff.

[42] United Nations Economic Commission for Europe, Guidebook on promoting good governance in public-private partnerships, New York - Geneva 2008, p. 13.

[43] KARPEN, U., Good Governance, European Journal of Law Reform, No 12 (2010), p 22.

[44] PRINC, M., Standardy dobrej administracji w prawie administracyjnym [Standards of good administration in administrative law], Wydawnictwo UAM, Poznań 2016, p. 17.

[45] APOSTOLACHE, M., Ch., The Constitutionalization of the Right to Good Administration and the Implications on Local Public Administration, Analele Universitatii Titu Maiorescu, Seria Drept, (2015) - Anul XIV, p. 28.

[46] The Voivodship Administrative Court in Gdańsk in the resolution of 5 May 2016, Case No. III SA/Gd 703/15.

[47] The Voivodship Administrative Court in Gorzów Wielkopolski in the resolution of 16 September 2008, Case No. II SA/Go 358/08.

[48] The Voivodship Administrative Court in Szczecin in the resolution of 16 November 2005, Case No. II SA/Sz 705/05.

[49] The Supreme Administrative Court in the resolution of 14 December 2017, Case No. I FSK 102/16.

[50] The Voivodship Administrative Court in Warsaw in the resolution of 13 December 2017, Case No. IV SAB/Wa 210/17.

[51] CHESHMEDZHIEVA, M., The Right to Good Administration, American International Journal of Contemporary Research, Vol. 4, No. 8 (2014), pp. 64-67.

[52] HOLZER, M., ZHENG, Y., Best Practices in E-Governance: A Comparative Study Based on the Rutgers University Worldwide Digital Governance Survey, in: Reddick, Ch. G., Anthopoulos L. (ed.), Information and Communication Technologies in Public Administration. Innovations from Developed Countries, CRC Press, Boca Raton 2015, p. 32.

[53] SUPERNAT, J., Zasady dobrej administracji [Principles of good administration], in: Niewiadomski, Z., Cieślak, Z., (ed.) Prawo do dobrej administracji, Materiały ze Zjazdu Katedr Prawa i Postępowania Administracyjnego, Warszawa-Dębe 23–25 września 2002 [Right to good administration. Materials from the convent of Law and Administration Procedure Faculties Warszawa-Dębe 23-25 September 2002], Wydawnictwo Uniwersytetu Kardynała Stanisława Wyszyńskiego, Warsaw 2003, p. 598-615.

ECOHESION: HOW TO MEASURE THE MAIN DRIVERS OF ADMINISTRATIVE BURDEN REDUCTION

Tamás Laposa[1]

DOI: 10.24989/ocg.v331.4

"The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the *Győző Concha Doctoral Program*

Abstract
This paper presents a new approach to measure the effects of e-government concepts on the reduction of administrative burdens, in the domain of European fund management.

The topic may receive considerable interest since the present European legislation specifies that Member States shall provide online portal services and offer paperless fund management possibilities for beneficiaries in order to reduce the administrative burdens of cohesion policy. This concept is marked with the term "eCohesion" in the scientific discourse. Based on former studies, the concept has several micro- and macro-level attributes that leverage its effectiveness and impact on burden reduction. Nevertheless the level of their influence has not been underpinned by evidence based research yet. Consequently this paper outlines a research design for the measurability and impact assessment of the above attributes.

The development of the research design is based on the Standard Cost Model, the widely-used methodology for the measurement of administrative burdens. The present paper applies the model to the attributes of eCohesion by formulating research hypotheses in order to make them measurable and to assess their relevance. The design created paves the way for a further quantitative research and methodologically supports Member States in developing a deeper understanding of the nature of eCohesion.

1. Introduction

According to Regulation 1303/2013 of the European Parliament and of the Council the EU provides funds for EU Member States through multi-annual development programmes in order to implement the Union strategy for smart, sustainable and inclusive growth, as well as the Fund-specific objectives including economic, social and territorial cohesion. Pursuant to the legislation arrangements for the implementation and use of the funds shall take into account the overall aim of reducing the administrative burdens on beneficiaries and bodies involved in the management and control of the programmes. [4]

With regard to these provisions the Commission started the eCohesion initiative to contribute to the reduction of administrative burdens and the effective implementation of the funds. eCohesion is a set of procedural, legal, technological and organisational components to support the provision of effective e-Government services. However the maximisation of efficiency gains depends on the

[1] National University of Public Service, Budapest

decisions of Member States, since the European legislation sets minimum requirements for electronic services. As proven by the study of the European Commission and Deloitte, efficiency gains can be realized at different levels and the rate of improvements can be significant. [3]

According to former studies four micro-level attributes (portal functionality, only once encoding, interoperability, one stop shop) and two macro-level attributes (procedural complexity, extent of funds) were identified which are relevant from the perspective of eCohesion efficiency. Nevertheless the level of their influence has not been underpinned by evidence based research yet. [9]

This paper has two main aims: first, to review the methodological and regulatory background of eCohesion and the reduction of administrative burdens; second, to formulate hypotheses that support the impact assessment of the above attributes of eCohesion.

2. The eCohesion concept

In 2007, the European Commission launched the Action Programme for Reducing Administrative Burdens in the EU to simplify administrative requirements and eliminate unnecessary administrative burdens on businesses, small businesses in particular. The Action Programme aimed at a 25% reduction of burdens by 2012. The Action Programme identifies 13 priority areas for administrative burden reduction. Cohesion policy is one of the priority areas where the calculations of experts estimated a 24% reduction of administrative costs. This amount corresponds to 0.7% of the total reduction of costs planned in the Action Programme. [1]

To reach the set targets, the Commission started an initiative (eCohesion) focused on the reduction of administrative burdens of cohesion policy and also rural development policy by streamlining the information obligations of beneficiaries and the provision of electronic data exchange services via online portals. The Commission and the experts of the Member States assessed the impacts, IT implications, specificities, costs and benefits of the proposal and established the detailed technical definitions of electronic services. ECohesion is not simply an IT issue. It also has to address a wide range of legal, procedural, organizational and Member State-specific factors. It is a framework of specific components to reduce administrative burdens via the implementation of e-Government services. The Commission drafted the legal requirements of the implementation of the concept. These requirements were included in the legal provisions of funding in the 2014-2020 period. [3]

Regulation 1303/2013 of the European Parliament and of the Council specifies the *three fundamental components of eCohesion*. The *provision of electronic data exchange services, interoperability of systems and the implementation of the only once encoding princ*iple ensure the reduction of administrative burdens. These components have a direct impact on the reduction of administrative burdens. The digital nature of the procedures requires specific conditions to guarantee the quality, effectiveness and the authenticity of services. For this reason the fundamental components need to be supplemented by *collateral components* such as *e-signature, e-document management and e-audit and interoperability*. These components have no influence on burden reduction but they are prerequisites of the fundamental ones.

Interoperability has a special nature as a dual component as it plays a role in both categories. *Figure 1* provides an overview of the structure of the components.

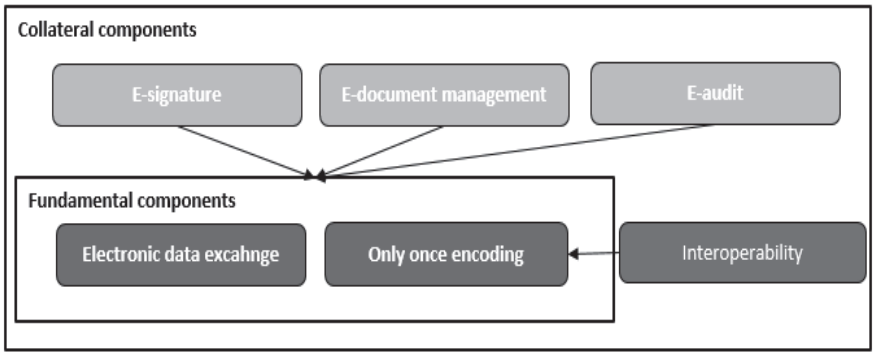

Figure 1: The framework of eCohesion

The detailed rules of the six components of eCohesion are specified by further implementing acts of the Commission (Implementing Regulation (EU) No 1011/2014; Implementing Regulation (EU) No 821/2014). These details are covered in the next sections of the article.

2.1. Electronic data exchange

Electronic data exchange systems are defined by the regulation as mechanisms and instruments allowing the electronic exchange of documents and data, including audio-visual media supports, scanned documents and electronic files. Member States shall ensure that all exchanges of information between beneficiaries and the relevant authorities can be carried out by means of electronic data exchange systems. The realization of electronic data exchange has a series of procedural, technological and legal requirements. The above European acts define minimum requirements that ensure the expected efficiency gains, but the requirements need to be adapted to national specificities and further particularized by national legislation.

The scope of electronic data exchange covers all exchanges of information including reporting and financial procedures as well as management verifications and audits. This ensures that reduction of administrative burdens can be realized to a full extent in case of projects with a grant agreement. That is to say that eCohesion shall be provided for beneficiaries. It depends on national decisions to extend these services to enable the submission of applications for support as well. According to the text of the regulation, eCohesion is compulsory for the Member States, but it is optional for the beneficiaries, unless the compulsory use of electronic data exchange systems is prescribed by national law. In this case, it shall be ensured that paperless procedures do not restrict access to the funds or harm equal opportunities. If a Member State applied compulsory eCohesion services in the previous programming period, this practice can be maintained without further requirements. The format of data and documents submitted electronically can be defined by national legislation and the detailed terms and conditions of electronic data exchange shall be laid down in the grant agreement concluded with the beneficiary.

Taking into consideration the full-electronic nature of procedures, the legislation sets specific technological requirements to guarantee the quality of services and the efficiency of procedures. The regulations lay down requirements on security, system availability, data integrity, data protection and privacy, methods of authentication and the minimum functionality of electronic portals.

2.2. The "only once encoding" principle and interoperability

Data and documents regarding a single development project shall be shared and re-used by the authorities involved in the management of the same development programme. The relevant authorities cannot ask for the same data repeatedly. This provision is without prejudice to cases when authorities need an update on erroneous or obsolete data or unreadable documents. The regulation sets the cooperation of authorities at programme level as a minimum requirement. This measure avoids multiple data requests during the life-cycle of a project, but it leaves the possibility open for Member States to manage different programmes in separate IT systems.

The pre-requisite of only once encoding is the seamless cooperation of relevant authorities and the interconnection of their information systems. For this reason the principle is strongly connected to the interoperability component of eCohesion. According to the European Interoperability Framework interoperability can be defined as "*the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems*". [2] Interoperability is not simply a technological issue. It requires the cooperation of authorities at legal, organizational, semantic and technical levels. [1]

As interoperability is strongly interlinked with the only once encoding principle, it shall be realized at least at programme level. Nevertheless it does not exclude the extension of interoperability to other databases which can bring further efficiency gains and extend the scope of burden reduction.

2.3. E-signature

As electronic data exchange transactions are carried out digitally an adequate level of authentication is required to guarantee the veracity of transactions. The required level of authentication depends on national laws and requirements on verification and audit. The regulation sets internationally-accepted standards here as well and leaves the definition of adequate levels to Member States. In pursuance of the legislation transactions shall bear an electronic signature compatible with one of the three types of electronic signature defined by Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. [5]

2.4. E-document management and electronic audit

The digitalization of procedures changes the nature of document submission and management. These procedures can bring about the desired benefits of burden reduction if they provide optimal conditions for auditors and relevant authorities as well. These changes have a series of technological implications. Since the vast majority of documents will be available in digital version only, IT systems shall be equipped with adequate document management capabilities enabling relevant authorities to process digital contents effectively.

To meet audit and verification requirements, the types of accepted data carriers and the compliance criteria of digital documents shall be laid down by national authorities on the basis of national legal requirements and audit standards. In addition, information systems shall meet accepted security standards to ensure the compliance with above legal and audit requirements. [6, 4] On the other hand, auditors cannot place paper-based obligations on beneficiaries in any case. Pursuant to the

implementing acts digital documents are reliable sources for audits and financial verification if they have been submitted via the electronic data exchange system. According to these provisions, paper-based originals cannot be required in case of every operation, only in exceptional cases based on a risk analysis.

3. The measurability of administrative burdens

Beneficiaries and applicants are subject to a series of legal obligations set by cohesion policy regulations. This is done to ensure the conditions of smooth and effective management of EU funds as well as to guarantee the realization of the underlying policy objectives. If the implementation of regulations impose unnecessary regulatory costs on businesses and citizens it is regarded as a socio-economic waste. It is crucial to constantly monitor and keep the balance between the benefits of regulatory requirements and their costs respectively. Administrative cost and burdens are important indicators of the business environment and their optimization can have a significant influence on overall economic competitiveness and productivity. [1, 10]

The costs of regulation can be split into three categories: *direct financial costs (financial obligations to transfer money), long term structural costs (long term effects of regulations on living and business environment) and compliance costs (behavioural and information obligations to comply with legislation)*. Compliance costs can be divided into indirect financial costs (costs of behavioural obligations) and administrative costs (costs of information obligations)

By the definition of the Standard Cost Model manual "*administrative costs are defined as the costs incurred by enterprises, the voluntary sector, public authorities and citizens in meeting legal obligations to provide information on their action or production, either to public authorities or to private parties*." Administrative costs are the costs of administrative activities related to the collection and provision of information. Nonetheless certain types of information would be collected by beneficiaries even in the absence of regulation. This triggers the introduction of the notion of *administrative burdens which are the administrative costs of information obligations imposed by legislation*. [7, 10]

From the perspective of regulations some of these burdens are necessary to meet the underlying policy objectives. There are some burdens however, whose removal would not jeopardise the realization of those policy objectives. Consequently, *the reduction of administrative burdens is focused on the elimination of these unnecessary administrative burdens*. [1]

The linkages between the different types of administrative costs and burdens are depicted by *Figure 2*.

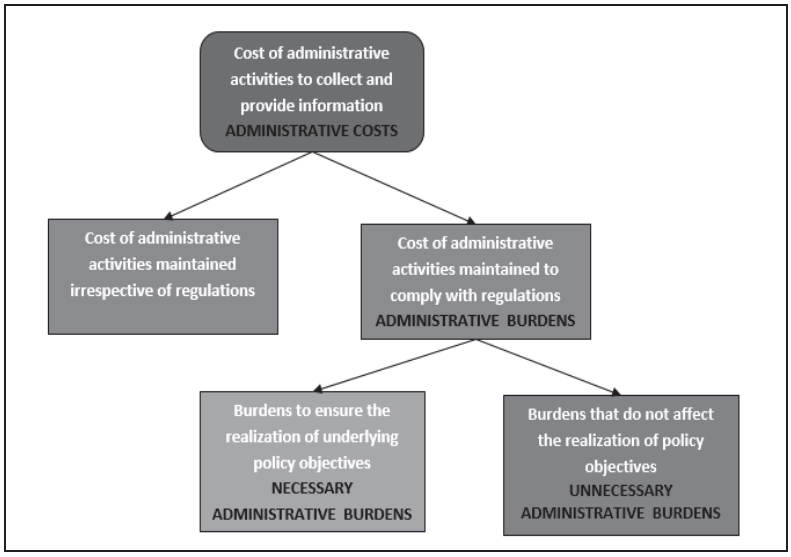

Figure 2: Types and relations of administrative costs and burdens

In order to reduce administrative burdens they need to be measured first. The Standard Cost Model is a widely-used methodology to measure the administrative costs of regulations. It has been designed to provide a clear-cut and consistent method to identify and measure administrative costs. The SCM can be utilized in different policy areas and it provides coherent and comparable estimates. The methodology is focussed on administrative activities imposed by regulation to fulfil information obligations.

The SCM makes the costs of activities measurable by breaking down regulatory requirements into manageable components. These components are the *cost parameters (Time, Price, Quantity, Frequency and Population)* of the relevant administrative activities. Price represents the hourly wage and overhead costs of activities. Time indicates the amount of time needed to complete the relevant activity. Quantity shows the size of the population of beneficiaries affected and the yearly frequency of the activity. The combination of these elements gives the basic SCM formula which is shown by *Figure 3*. [10]

Cost of an administrative activity = Time x Quantity x Price
Quantity = (Population x Frequency)

Figure 3: The SCM formula [10]

By using the above formula the costs of different administrative activities and the administrative burdens of beneficiaries can be calculated. The formula also helps decision makers to reveal the cost structure of single administrative activities. Since the above cost parameters are the basic elements of activities they can be the basis of different kinds of burden reduction. Administrative burdens can be reduced in different ways either by concentrating on single cost parameters (e.g. reducing time or frequency) or their combinations.

The Action Programme for Reducing Administrative Burdens comprises a list of burden reduction principles to guide Member States in cutting red tape in Europe. These principles and their main cost parameters are listed on *Table 1*.

rinciples	Cost parameter
Reduce the frequency of reporting requirements to the minimum levels necessary to meet the substantive objectives of the legislation	Frequency
Review whether the same information obligation is not requested several times through different channels and eliminate overlaps	Frequency
Require electronic and web-based reporting where paper based information gathering is presently required	Time, Price
Introduce thresholds for information requirements, limiting them for small and medium sized companies wherever possible, or rely on sampling	Time
Consider substituting information requirements on all businesses in a sector by a risk based approach	Population
Reduce or eliminate information requirements where these relate to substantive requirements that have been dropped or modified since the information requirement was adopted	Time, Frequency, Administrative activities
Provide official clarification of complex pieces of legislation that may either slow down business activities	Time

Table 1: Principles of administrative burden reduction [1]

4. The main attributes of eCohesion

European legislation sets the minimum requirements of eCohesion that ensure the expected level of burden reduction. These requirements need to be adapted to national specificities and further particularized by national legislation. It is the decision of each Member State to adopt the minimum framework of requirements or to go beyond them. This means that the eCohesion solution and the level of total efficiency gains may differ from country to country. [5] If a country decides to exceed the minimum requirements and develops more sophisticated portal functions they can reach higher levels of burden reduction. Thus, burden reduction has different stages that can be achieved according to the decisions of Member States. The European Commission and Deloitte elaborated a maturity model to measure the sophistication of eCohesion portal functionalities and potential efficiency gains. Based on this model *an annual 8 % of administrative burden reduction could be estimated, if the highest level of portal sophistication would be implemented* in all EU Member States. [3]

The above model provides a good roadmap for Member States to plan the development of eCohesion portals but it dominantly focuses on the functionality of e-portals. It is reasonable to assume that the success of burden reduction is influenced by a wider range of attributes, however. In the course of former studies, the concept of eCohesion was analysed to reveal its main attributes influencing the reduction of administrative burdens. Based on these studies eCohesion has the following micro and macro level attributes. [8]

As stated above, eCohesion has two types of components. The fundamental components take a direct effect on burden reduction and collateral components (*e-signature, e-document management, e-audit*) are not linked to efficiency gains but they create the essential conditions for the fundamental ones. As the interoperability component has a special nature, its role will be further discussed below.

In terms of *portal functionality* Regulation 1011/2014 prescribes that electronic data exchange systems shall be equipped with at least the following functionalities: interactive forms and/or forms prefilled by the system, automatic calculations, automatic embedded controls which reduce repeated exchanges of documents or information, system-generated alerts, online status tracking. [5] These functions are directly linked to the reduction of burdens and the issue of efficiency. The *principle of only once encoding and interoperability* are strongly interrelated. Their minimum requirements

ensure burden reduction within the limit of a single development programme. Here the efficiency of fund management can be further extended if a Member State applies these components for all development programmes. In case of interoperability, system connections to national databases and the automatic retrieval of relevant beneficiary data can further reduce burdens. The eCohesion concept does not restrict the usage of separate IT systems for the management of different programmes. This means there can be more than one eCohesion portal in a Member State. In this situation beneficiaries might need to use different portals for different types of projects which can complicate the administration of projects compared to the usage of a single e-portal for all funds. Hence the principle of *one stop shop* can improve the efficiency of eCohesion.

The above four attributes (*portal functionality, only once encoding, interoperability, one stop shop) are labelled as micro-level attributes of eCohesion*. These attributes contribute to the reduction of administrative burdens from a technological perspective. Nevertheless there are some further *macro-level attributes* that define the organizational and economical context of eCohesion.

The main procedural guidelines of EU fund management are set by European legislation but they need to be applied in a national administrative and organizational context. Each Member States has specific administrative structures (number of administrative levels, number of agencies, extent of territorial decentralization) which produces a different procedural complexity in each country. Procedural complexity defines the scope of administrative activities and information obligations i.e. the main building blocks of administrative burdens. Thus, *procedural complexity defines the boundaries of burden reduction.* EU funds represent different economic weight in each Member State. It is rational to assume that the extent of funds and the number of potential beneficiaries can have a definitive impact on the approach of a country to the eCohesion concept and the targeted reduction of administrative burdens. In case of a low funding budget, the potential IT budget can be rather small or funds can reach a moderate group of beneficiaries which can limit the potential scale of burden reduction. Consequently, the *magnitude of the available funds* need to be taken into account when evaluating the effects of eCohesion.

5. Research design development

Former studies highlighted the importance of the above micro and macro attributes but their relevance and the extent of their influence has not been underpinned by empirical research yet. This paper aims to outline a research design for the impact-assessment of these presupposed attributes. Since eCohesion is targeted at the reduction of administrative burdens, the desired research should be based on the methodological foundations of burden reduction. This article examines the relevance of the identified attributes by utilizing the methodological building blocks of the Standard Cost Model, as an internationally-accepted method for the measurement of administrative costs.

In an attempt to verify the relevance and the effects of the presupposed attributes, their relationships with the different elements of the SCM formula (*Number of administrative activities, Time, Price, Frequency, Population*) will be analysed (*Phase 1*). By identifying these potential linkages, some research hypotheses will be defined (*Phase 2*) to support the impact-assessment of the attributes (*Phase 3*). This paper encompasses Phase 1 and 2, the above impact-assessment will be realized in the framework of further studies.

5.1. Linkages between attributes and SCM elements

Micro-level attributes have a technological impact on the management of prescribed administrative activities. Electronic tools do not change the number of prescribed administrative activities and the scope of clients affected by them (Population) as they are defined by regulations. Nor can they change the hourly price of activities since they are influenced by economic factors. Their most significant advantage is that they can simplify procedures and decrease incorrect data processing by built in checks and warnings. It is reasonably assumed that they accelerate procedures and they can prevent repetitive and parallel data exchange. Consequently, *this study suggests that micro-level attributes have an effect on the lead times of administrative activities and the frequency of data exchanges*.

The findings of the European Commission and Deloitte justified the assumption that a higher level of portal sophistication can bring about a remarkable burden reduction. The minimum functionality set by the legislation is focused on a higher level of portal usability, the acceleration of data processing and the reduction of repeated corrective data exchanges by automatization and embedded controls. This can have a real impact on lead times and the frequency of activities.

The application of the only once encoding principle nullifies parallel information obligations by prescribing the re-use of already submitted data for all authorities implementing the same programme. This measure hinders relevant authorities to ask for the same data from beneficiaries and prevents any authority to ask for the data in different formats. Accordingly only once encoding has an undoubted influence on the frequency of data submission. The eventual extension of only once encoding across different programmes may ensure the re-use of any data or document submitted by the beneficiary. This extension provides an extraordinary opportunity to automatize data processing, having a special effect on the lead time of activities.

Pre-filled data and the re-use of already submitted data decreases the scope of data requirements. The same goal can be realized if Member States utilize public data registers for this purpose. Establishing data connections to external public databases Member States can have access to valid information without data exchange with beneficiaries. The interpretation of interoperability as a fundamental component of eCohesion and the limitation of data requirements provide an opportunity to accelerate data submission (*Time*) and further minimize the likelihood of repeated corrective exchanges (*Frequency*).

The registration of separate accounts on different portals and the knowledge of several user interfaces require more effort from beneficiaries. Tracking changes and notifications in different portals complicates administrative activities. It is conceivably hypothesized that users need to spend more time on the management of administrative activities in this case, so a single one stop shop portal could also represent a remarkable opportunity of simplification.

Macro-level attributes represent organizational, procedural and economic conditions. *This study assumes that macro-level attributes exert influence on wider scope of elements of the SCM formula.* Procedural complexity has an impact on the general setup of administrative activities. Legislation defines the range of activities (*Number of activities*), the frequency of periodic and repetitive data exchanges (*Frequency*), the scope of data requirements and electronic documents to be submitted (*Time of data processing*).

In case legislation makes eCohesion optional for beneficiaries, relevant authorities need to maintain parallel paper-based procedures. Paper-based procedures lack the main advantages of electronic applications i.e. the chance to automatize data submission and the control of correct data processing. As these characteristics can have a remarkable effect on the time and frequency of administrative activities, it is thus suggested that the optionality of eCohesion affects efficiency negatively. As seen above procedural complexity influences almost all elements of the SCM formula. The only exception here is the hourly price of activities that is defined by further factors beyond the scope of this research.

The magnitude of the available funds may define the attitude and motivations of Member states towards the issue of burden reduction realized by eCohesion. The size of the funding envelope determines its potential economic impact, and the level of funds available for the development of eCohesion portals. Therefore it is hypothesized that these conditions might have an effect on the targeted level of burden reduction.

The above findings seem to confirm the assumptions that micro-level attributes influence the time and frequency of administrative activities and macro-level attributes impact almost the complete range of SCM elements. The findings of the study are summarized by *Table 2* below.

eCohesion attribute	SCM formula elements	Relationship
Portal functionality	Time, Frequency	Usability of user interfaces, automatization and embedded controls simplify data processing and reduce repeated corrective exchanges.
Only once encoding	Time, Frequency	The re-use of submitted data decreases parallel data submission and accelerates the completion of subsequent activities.
Interoperability	Time, Frequency	The retrieval of valid data from other databases substitutes data submission and prevents corrective exchanges.
One stop shop	Time	The usage of different accounts makes the management of activities complicated
Procedural complexity	Time, Frequency, Number of activities, Population	Procedural complexity determines the general setup of administrative activities
Magnitude of funds	Administrative burdens	The magnitude of the available funds influences the attitude to the issue of burden reduction

Table 2: Relationships between eCohesion attributes and SCM elements

5.2. Formulation of research hypotheses

The identified linkages between the presupposed attributes and the SCM formula supports the formulation of research hypotheses to assess the relevance and the extent of the single attributes. These hypotheses make the attributes measurable and paves the way for further phases of the research design. Utilizing the relationships between attributes and SCM elements the paper aims to establish at least one hypothesis for the measurement of each eCohesion attribute.

Hypothesis 1: Many aspects of the single micro-level attributes are connected to reduction of data requirements. Automatization of data processing, the re-use of already submitted data as well as the retrieval of valid data from public registries accelerate data processing (*Time*). It is thus hypothesized that *the reduction of number of data and documents required influences burden reduction favorably.*

Hypothesis 2: User-friendly portal functions facilitate the management of administrative activities. Irrespective of the number of data requirements easier navigation, quick access to frequently-used functions and user-centric interfaces can accelerate data processing (*Time*). *It is therefore suggested that higher levels of user-friendliness also have a positive effect on administrative burdens.*

Hypothesis 3: the consequence of the usage of multiple fund management portals is that beneficiaries need to use diverse functionalities for different project types. According to the approach of this study, usability is an important driver of efficiency. The parallel development of systems results in a heterogeneous usability of eCohesion portals and it has an influence on efficiency gains. *Hence it is argued that the parallel usage of portals requires more time from users and has a negative effect on burden reduction.*

Hypothesis 4: Correction of mistakes of data processing result in the repetition of administrative activities and increase the frequency of data submission. Measures preventing these repeated exchanges represent a significant resource in the simplification of administrative procedures. The above objective can be achieved either by narrowing the scope of data requirements (*automatization, re-use, retrieval*) or by embedded controls. *The paper assumes that the prevention of corrective actions provides an exceptional opportunity to reduce administrative burdens.*

Hypothesis 5: information technology can boost the efficiency of administrative activities by changing the gap between total (*all data needed*) and absolute (*data effectively entered*) data requirements. It is apparent that the main determinant of administrative burdens is the total number of data requirements, nevertheless. The total number of data might have a significant influence on the frequency of corrections as well. *It seems thus reasonable to hypothesize that the main driver of burden reduction is the simplification of procedures.*

Hypothesis 6: the economic impact of the funds can differ from Member State to Member State. Taking into account the diverse economic weight of funds governments might develop a different approach to utilize the potential of eCohesion to reduce administrative burdens. This can have a serious impact on the IT budget of the Member State and the sophistication of portal functionalities. As discussed above, functionality is linked to the Time and Frequency cost parameters, so the last hypothesis is indirectly connected to these SCM elements as well. *Therefore it is assumed that the targeted level of burden reduction is determined by the economic weight of the funds.*

Analysing the main drivers of the hypotheses it is reasonable to anticipate that the efficiency of eCohesion is cantered on the number of data requirements and controls as well as the usability of portal functionalities. As already pointed out in this paper the efficiency gains of eCohesion can be realized at different levels and their maximization depends on procedural, technological decisions of Member States. It has been assumed by former articles that efficiency of this concept is influenced by the above micro- and macro-level attributes. These hypotheses can be utilized to create a questionnaire in order to collect empirical data for their impact assessment.
As supposed by former studies efficiency levels of eCohesion could be best measured by a specific maturity model. The results of the above impact assessment and the identification of the relevant attributes of eCohesion efficiency can pave the way for further research and the creation of this eCohesion specific model.

6. Conclusion

The concept of eCohesion is aimed at the provision of e-Government services in order to improve the efficiency of funding procedures in the area of European cohesion policy and rural development policy. These efficiency gains can realize a significant reduction of administrative burdens. In addition to the European legal provisions national regulations can further extend the level of efficiency gains.

Based on former studies four micro-level attributes (portal functionality, only once encoding, interoperability, one stop shop) and two macro-level attributes (procedural complexity, extent of funds) were identified which are relevant from the perspective of efficiency. The relevance of these attributes has not been clarified by evidence-based research yet.

In an attempt to verify the relevance and the effects of the presupposed attributes this article utilized the Standard Cost Model, an internationally-used methodology to measure administrative costs. Based on this model, this article identifies linkages between the above attributes and the measurable components of administrative activities. These linkages facilitated the formulation of the following six research hypotheses to support the impact-assessment of the attributes: *the reduction of number of data and documents required influences burden reduction favourably; the level of user-friendliness leverages burden reduction; the prevention of corrective actions has a remarkable impact on administrative burdens; the usage of multiple portals drives down efficiency; the main driver of burden reduction is the simplification of procedures; the targeted level of burden reduction is determined by the economic weight of the funds.*

These hypotheses can be utilized to conduct a questionnaire-based impact assessment on the relevance of the presupposed attributes. The results of this assessment and the identification of the relevant attributes of eCohesion efficiency can open new fields of research to create a specific model for the measurement of efficiency levels of eCohesion.

7. References

[1] EUROPEAN COMMISSION, Action Programme for Reducing Administrative Burdens in the EU, Office for Official Publications of the European Communities (Pages 3, 8), Luxembourg 2010.

[2] EUROPEAN COMMISSION, European interoperability framework EIF) for European public services (Pages 1, 2), in: Official Journal of the European Union, Brussels 2010.

[3] EUROEAN COMMISSION, eGovernance study at EU / Member State level, Draft final report by Deloitte, (Pages 14 – 15, 48), Brussels (2012), Viewed 5 January 2017, [online]. http://ec.europa.eu/agriculture/external-studies/2012/e- %20government/fulltext_en.pdf

[4] EUROPEAN COMMISSION, Regulation (EU) No 1303/2013 of the European Parliament and of the Council (Articles 4, 122, 140), in: Official Journal of the European Union, Brussels 2013.

[5] EUROPEAN COMMISSION, Commission implementing regulation (EU) No 1011/2014 (Chapter II.), in: Official Journal of the European Union, Brussels 2014.

[6] EUROPEAN COMMISSION, Commission implementing regulation (EU) No 821/2014 (Chapter III.), in: Official Journal of the European Union, Brussels 2014.

[7] JOEY VAN DEN HURK, Standard Cost Model for Citizens - User's guide for measuring administrative burdens for Citizens, Ministry of the Interior and kingdom Relations, Hague 2008.

[8] LAPOSA, T., The digital transformation of E- cohesion policy, NISPA CEE, Kazan 2017.

[9] LAPOSA, T., eCohesion maturity: How to measure the efficiency of digital cohesion policy, Central and Eastern European e|Dem and e|Gov Days, Budapest 2017.

[10] SCM NETWORK, International Standard Cost Model Manual - measuring and reducing administrative burdens for businesses, (Chapter 3), 2005. Viewed 5 January 2015, [online]. http://www.administrative-burdens.com

Workshop on Smart Cities, Council of Europe I

ELEMENTS OF LOCAL AUTONOMY AND NEW TECHNOLOGY IN URBAN REVITALIZATION PROCESS

Anastasia Stefanita[1]

DOI: 10.24989/ocg.v331.5

Abstract

The article aims to present the concept of the urban revitalization in relation with the new information technologies. The actuality of the topic relates from the importance of information tools in all processes of human activity, including the administrative and participatory one. The urban revitalization is presented as a dimension of the decisional local autonomy of public authorities of the cities/municipalities. The paper is based on the on-going activities of the bilateral Polish - Moldavian "Revitalization Project". The e-tools become a new dimension of the classical "renewal" concept, transforming in this way the revitalization process in a modern one and upgrading it to a higher level. Because of the rapid development of the information society, the revitalization processes undergo changes and gains new meaning. The expectations of citizens as well as the activities of local public authorities imply new standards, especially in terms of information technologies.

1. Definition and concept of urban revitalization

1.1. The notion of urban revitalization

There are several terms and definitions of urban revitalization. In the United Kingdom the process is called „urban regeneration", but in United States – "urban revitalization". Also in the literature we will find the notion of "urban renewal".

Urban renewal or urban regeneration is a broad term referring to special local development actions and programs aimed at upgrading run-down urban areas. More recently, the term has also come to cover the general objectives of 'integration' or 'social inclusion', though the precise interpretation of these notions may vary from context to context. [11]

Modern attempts at renewal began in the late 19th century in developed nations, and experienced an intense phase in the late 1940s under the rubric of reconstruction. The process has had a major impact on many urban landscapes, and has played an important role in the history and demographics of cities around the world. Urban renewal has been seen by proponents as an economic engine and a reform mechanism, and by critics as a mechanism for control. It may enhance existing communities, and in some cases result in the demolition of neighbourhoods. [21]

Urban renewal can be regarded as a tool for public policies reacting to the complexity of urban development [5]. Broadly defined, urban renewal can encompass all public and private efforts to improve city form and life. [9, p.212]

[1] Solidarity Fund PL in Moldova, Chisinau; Information Society Development Institute, Chisinau, Republic of Moldova; PhD student Academy of Public Administration, anastasia.stefanita@gmail.com

The Revitalization Law of Poland no.1777 of October 9, 2015 defines urban revitalization as "the process of bringing out degraded areas from a crisis state, conducted in a comprehensive way, through integrated actions for the local community, space and economy, geographically concentrated, run by revitalization stakeholders based on the municipal revitalization program".[12]

The urban revitalization should have a legal base: it can be a law but it is facultative, or another kind of document (Government Decision, Public Policy, Strategy, etc.). At the local level, the city/municipality should develop their Revitalization Program that is a more practical document (including a portfolio of concrete actions – projects ideas) including as well the vision and strategically measures to be taken in order to develop the city through a concrete identified area.
A key element of the urban revitalization is identifying the most degraded area/sector of the city. The degradation do no refers only to the state of the infrastructure, but as well to the social situation (level of unemployment, deprived people, alcoholism, etc.).

The various dimensions of urban life – environmental, economic, social and cultural – are interwoven and success in urban development can only be achieved through an integrated approach. Measures concerning physical urban renewal must be combined with those promoting education, economic development, social inclusion and environmental protection. It also calls for strong partnerships between local citizens, civil society, industry and various levels of government. Such an approach is especially important at this time, given the seriousness of the challenges European cities currently face, ranging from specific demographic changes to the consequences of economic stagnation in terms of job creation and social progress, and to the impact of climate change. The response to these challenges is critical for achieving the smart, sustainable, inclusive society envisaged in the Europe 2020 Strategy. EUR 371 million is set aside for innovative actions in the field of Sustainable Urban Development over a seven-year period (2014 – 2020). [10] In this way, urban revitalization is becoming a priority of the European Union, including financial programs and instruments.

Over the past decade or so, a potentially more powerful theory for city and regional growth has emerged. This theory postulates that people are the motor force behind regional growth. Its proponents thus refer to it as the "human capital" theory of regional development. [6, p.32] In this context, we would like to define the urban revitalization as a process of cities/municipalities development through efficient local partnerships, high civic engagement and the concentration of resources in a certain area considered the most degraded in order to solve social problems of the community and bring a change with a high social impact.

1.2. Urban revitalization and local autonomy

In the context of the current research, the process of urban revitalization can be analysed as a dimension of the local autonomy, too. More concretely, it is a form of decisional autonomy. As was mentioned above the urban revitalization is a process based on efficient partnerships at local level. It means that local public authorities should establish partnerships with all stakeholders: business sector; civic society; citizens; other public institutions and other potential partners at the local level. As well, local authorities are free to cooperate with regional structures (for example Regional Development Agencies in the Republic of Moldova) in order to receive support in urban revitalization process, or even national/central authorities (ministries, agencies, etc.) and international donors/partners.

In this respect, the level of local decisional autonomy should be high to facilitate in this way the creating constructive and functional partnerships.

The general local administrative autonomy is highlighted as one of the basic principles of the revitalization process. It is absolutely applied in the resource prioritisation and provision process, both: the public-administrative resources and the private or community resources identified for implementation of the revitalization activities.

The owner and the leader of the revitalization process is the local public authority (e.g. mayoralty), that's why it should have a real functional local autonomy in all dimensions and fields. Obviously, there are legal limits that should be respected but the main goal in the case of urban revitalization is the local development and a better life for citizens.

The history of urban revitalization in the United Stated involves complex interaction among the institutions, actors, and resources of both the public and private sector. Municipalities in the .U.S are somewhat autonomous and self-sufficient, especially since achieving "home rule" during the Progressive era of the early 19s. While this decentralized arrangement allots most land use authority to the municipalities, they are also obliged to provide a wide array of essential services to their residents using locally generated revenue. Despite having these robust responsibilities for the well-being of their citizens, however, cities' economic and physical developments have been overwhelmingly driven by private investment. Even the most aggressive attempts by government to direct urban revitalization have been geared toward providing optimal conditions for the private development of property. [22, p. 22]

Talking about Europe and different administrative systems (especially from the local autonomy perspective and the level of centralism), urban renewal is an important objective of public policies in European countries (e.g. France, Netherlands, Germany, UK, etc.). For example, in France and the Netherlands, central government involvement in urban renewal is evolving from direct intervention through sectoral subsidies, towards a "territorialized" policy. Funding for urban renewal is made available for local planning authorities in contracts with central government. These contracts are based on territorial strategies elaborated at the local level. This takes place in a context where the role of the public sector is changing. Local planning authorities become more autonomous and depend to a lesser extent on central government. At the same time, they develop a more business-like approach towards co-operation with private bodies. [23]

Besides the right of local autonomy, local authorities should have enough capacity and responsibility to manage all local issues, including an efficient cooperation relation with the business sector and other stakeholders. In ex-soviet countries, e.g. Republic of Moldova, the local autonomy is discussed more from the perspective of the rights and not – resources and real capacities. During last years, due to European integration aspirations, Moldova is promoting more active on the political agenda issues concerning real autonomy functioning in the framework of the local public administration reform based on subsidiarity and local autonomy principles.

In the same context, disinvestment, population loss and the phenomena of urban crisis that result are well known in cities all over the world, but especially in ex-soviet countries (e.g. Moldova a small country of approx. 3 mln. inhabitants, where emigration is a phenomenon - approx. 106 people are leaving daily the country [16]). More than one in four cities around the world were found to be shrinking cities between 1990 and 2000 [17]. Thus, while some cities prosper and attract people and investments, others fail to do so and experience deindustrialization, population loss and decay

instead. The burdens of decline are, however, not carried by a handful of unfortunate peripheral cities only, but are increasingly becoming a fairly 'normal' pathway of urban development. For municipal/local governments, population losses are associated with numerous economic, fiscal, infrastructural and social problems. When jobs are lost and residents leave the city, the result is a downturn in the income available for the maintenance of urban infrastructures such as schools, houses, water networks, cinemas and grocery stores. As a result, these infrastructures become underutilized and under maintained, and often have to be abandoned. With a declining number of residents and less business to tax, local government revenues are under stress, and the ability of local government to cope with the difficulties is seriously impaired. Moreover, high unemployment leads to all kinds of problems and a need for social services that can hardly be met with limited resources. [4, p.754-755]

Urban revitalization is becoming a potential solution for this problem: by revitalising unused and underutilised spaces and turning them into places people want to live, work and play in, in order to deliver spaces that are functional, enjoyable and foster genuine connection between people and place. On another hand, urban revitalization is a good solution for another big challenge of local administration when migration from rural to urban space is high and there are overpopulated cities - revitalization of peripheral areas.

Following from this, local governance arrangements need be understood as a complex interplay of macro-spatial conditions and local dynamics. [4, p.757] Also, the restructuring of nation-states and of the economy has created space for subnational mobilisation, especially at city level. [15, p.178] It is generally argued that although cities and states were highly interdependent in Western Europe, and to some extent becoming more and more so, many cities (in the sense of collective actors) have acquired and increasing sole in political and economic terms. [14]

1.3. IT tools and urban revitalization

Because, today, new technologies play an important, and sometimes even a central role in all human activities, IT tools do not miss from the revitalization, too. There are different ways of using e-tools within revitalization activities.

New tools created by the ICT industry have the potential to help city governments address the growing range of challenges that they are facing. Deploying ICT tools require a new discipline of digital urban renewal and a philosophy that incorporates both political leadership and open collaboration. [8, p.1]

IT tools are used efficiently from the early stage of the revitalization process. Because the communication with citizens is a very important aspect in any revitalization project, e-tools become a very useful method for achieving the main goal: communication and involving residents. This communication can be done more effective through web pages, social networks, text messaging, emails, text and video chatting, etc. Spreading important information concerning the revitalization activity to the entire community is easier to be done via electronic tools. Today is a must for all public authorities to have an updated web page where each citizen can access the necessary information on the city life. This is a transparency tool as well. Also, there are different mechanisms: electronic screens in the buildings, electronic billboards on the road in the city, mobile apps, etc. Social media is an actual way of mutual communication: authorities are publishing information and citizens interactively comments and participate in the discussion process.

To keep informed all stakeholders on the revitalization process, usually, authorities creates special dedicated web pages and pages on the social media tools, where regularly are posted photos, videos and other kind of reports (e.g. Starachowice city from Poland: http://rewitalizacja.starachowice.eu/en/ - web page and page on social networks https://www.facebook.com/starachowiceODnowa/). [19] Following each public/civic consultation process, the local authority publishes the results and decisions on the webpage with all notes and arguments.

Besides the fact that the technologies are an efficient communication tool, IT becomes a method of revitalization. Today is absolutely possible to transform the revitalized area in a high tech centre, which becomes a business focus. "Economic growth thus requires the presence of technology, talent, and tolerance" [22, p. 51], that in the urban revitalization context refers to IT tools for local government, social inclusion and openness to change, new and innovation.

Because the revitalization process is an intersectorial one, "people in science and engineering, architecture and design, education, arts, music and entertainment, whose economic function is to create new ideas, new technology and/or new creative content" [22, p. 51]

Therefore, information technology plays a much greater role in communication, entertainment, and retail than before, altering the nature of demand for urban space. And building technologies have advanced. [22, p. 3] Generally speaking, "to understand the development of revitalization policy, it is necessary to recognize the marked changes in technology, demographics, and settlement patterns that threatened the aging urban giants'.[22, p. 27]

IT tools have a big role in creation of the revitalization network. The experience of Poland shows that a unique web page – portal for all cities involved in the revitalization process (20 cities included in the national program plus 3 cities selected) is efficient to ensure the equitable and equilateral communication among all stakeholders and all cities.

Besides using ICT to make existing processes involving interaction between the municipality and citizens better, cheaper, or both, ICT has a big role referring to the economic-regional development: ICT-oriented economic development or regeneration. It aims at attracting digital industries or residents that make real estate decisions based on the availability of broadband. [8, p.19] Concerning resource management – an important task of local government, the use of ICT can facilitate the improvement of functioning citywide systems to use energy and other resources more efficiently. Local authorities are improving the publics service delivering via IT tools. Today we are using e-services in different sectors: health, education, social, etc. All these are becoming part of revitalization processes when coming to citizen's life improvement issue. From the community perspective, using ICT and crowd-sourcing conduct to increasing community cohesion, or influence and improve the political system. Typically started by civil sector organizations or social enterprises.

In the context of an increasing role of ICT in urban development process, new concepts and phenomenon occur. As a result, the smart city has emerged as approach to contemporary urban planning and sustainable development. The idea of the smart city or community has a center but no clearly defined boundary. There is not even a general agreed terminology, with "smart city", "intelligent city", "wired city", "senseable city," and "smart and connected community" all used to describe similar concepts [8, p.6] There are four characterisations of cities – wired, digital, intelligent, and ubiquitous – which gives a background to the emergence of the smart city. In effect,

it includes a digital infrastructure for communication, the ‘glue‘, which holds the services together and enables the usage. [7, p.47/p.55]

So as urban development needs integrated and systematic approaches, including urban revitalization, we can mention another new concept and approach: digital urban renewal. At the heart of all of the different approaches is a series of programs or concepts that are aimed at making life in cities better through the use of ICT. These programs and concepts are typically a combination of: environmental sustainability; economic performance; community cohesion; efficiency of operations and/or cost reduction. [8, p.6]

Despite the widespread enthusiasm for digital urban renewal and the availability of technologies, there has been relatively little progress. The most fundamental obstacle to digital urban renewal is the limitations of municipal government. Many city governments are neither empowered nor sufficiently resourced to carry out wide-scale digital urban renewal projects (challenges mentioned above in the context of local autonomy principle). The budgets, authority, geographical boundaries, and organizational structures of many municipal authorities belong to an earlier era, and unlike comparably sized businesses, city governments are under political constraints that prevent them from conducting comprehensive restructuring programs. In addition, many are already struggling with the magnitude and complexity of the day-to-day problems that they face. Multiple and contradictory objectives and lines of accountability to central government authorities and citizens make this even more difficult. Other barriers to the introduction of digital urban renewal programs can be attributed to a fear of change, both: civil servant and citizens. Digital urban renewal also raises concerns about privacy and civil liberties. [8, p.15-16]

Due to the increasing role of the new technologies, the urban revitalization is gaining new dimensions and methods of making changes at the local level in the context of modern tendencies and diversity of the challenges that local authorities have to face.

2. Urban revitalization in Republic of Moldova

2.1. Polish-Moldavian project on Urban Revitalization

For the Republic of Moldova, the notion and concept of urban revitalization is new. It was introduced with the launch of the project “Support of the public administration in Moldova in the implementation of regional policy through sustainable and integrated urban development” in July 2017. This project is designed for the period of two years: 2017-2019. The main goal of the project is the transfer of the Polish experience to Moldova in the field of urban revitalization, so as Poland has good practises in this sector and is open to offer a real support to Moldova.

The two countries have a good collaboration history. The countries established relations following the independence of Moldova at 1991. The similar history (both were occupied by Russia and Soviet Union in various times) makes the context of development appropriate and transfer of expertise very relevant. Poland is among the first ten commercial partners of Moldova. Poland has been providing assistance to Moldova in reforming its administration and economy and has supported Moldova on its path to integration into the European Union. Moldova has been a priority country of Polish development aid since 2004. The aid measures are executed in the framework of the Multiannual Development Cooperation Programme and several projects, which cover, among others: regional development and capacity building of the national and local administration.

The actual project is financed by the Polish Development Cooperation Program of the Polish Ministry of Foreign Affairs - Polish Aid 2017 and it is implemented by the Ministry of Economic Development of Poland in collaboration with Ministry of Agriculture, Regional Development and Environment of the Republic of Moldova with the local support of the Solidarity Fund PL in Moldova (Information Centre for Local Authorities).

The main beneficiaries of the project, at the local level, are 15 municipalities and cities. It is actually one of the first projects in Moldova that addresses to municipalities after the Law no. 764 from 27.12.2001 on administrative-territorial organization [13] was updated and approved a new list of 13 municipalities. The project includes 10 of them (besides Chisinau – the capital; Bender and Tiraspol – from the left bank of Nistru River). Additional to 10 municipalities, in the project were invited 5 more cities (Ialoveni, Cimislia, Causeni, Edinet, Briceni) that have a good potential of development based on the number of population, geographical position, capacity to attract funds and good experience in project implementation, as well as a presence of a big need of urban revitalization.

The project supposes creating efficient support system for effective urban development and renewal of cities, on one of the hands, and on another one - improving quality of development projects in cities including regulatory, institutional and financial instruments through developing, testing and piloting of programs and projects for urban regeneration.

The action includes two level interventions:

- at national and regional level - to provide technical assistance/policy advise to develop existed and/or draft new instruments and mechanisms dedicated to cities and renewal of cities and to implement them finally;

- at the local level - to provide advice and enhance skills for cities to develop and adopt urban renewal programmes and to identify and implement projects. [18]

The approach of the urban revitalization in the Republic of Moldova has two main directions that should go on in a parallel way. On one of the hand, there should be a bottom-up approach, cities having the main role in the implementation of urban revitalization process; and on another hand there is necessary to update and renew legal provisions by including the notion of urban revitalization in the legal framework, which is mainly under the responsibility of the Ministry of Agriculture, Regional Development and Environment of the Republic of Moldova. In this context, this parallel approach should conduct to revision and developing the legal and institutional framework and to the participative process through involvement all relevant stakeholders at local level.

Also, a central point is drafting the renewal programmes and projects at the cities level. Logically, based on the general-national legal framework that provides the general directions and priorities, cities and municipalities will develop their “Urban Revitalization Programs”. These plans are different than “General Urban Plans”. The main differences between these two plans, both very important for cities, are: General Urban Plan refers to the entire territory of the city but the Urban Revitalization Program is focused on a concrete area of the city - the most degraded sector; the General Plan is focused mostly on the infrastructure issues but the Urban Plan should be oriented to a high social impact. For drafting and implementing the Urban Revitalization Program is very important to establish efficient partnerships and to get involved the citizens. Also, involvement of

the local business sector in the process has a crucial role. Generally speaking, the General Plan has mostly the hard component, while the Revitalization one is focused on the soft one.

2.2. The readiness of cities and municipalities to undertake urban revitalization activities

The main goal of the revitalization process is to revive the identified depraved area not only from the infrastructure point of view but also from the social one. The objective is to attract people and to facilitate different processes, activities to be organised in this area. In this context, is very important the readiness of the cities to undertake urban revitalization activities.

Within the project, during August – September 2017, cities involved in the project activities, filled in a questionnaire. The goal of the activity was to obtain information from a local perspective - both on the functioning of regional development mechanisms at local level, as well as on the specific conditions of each locality, the achievements, the problems and the expectations in the context of the theme and the scope of the project.

The analysis of individual responses shows that the questionnaires were completed by people with different professional profiles and perhaps with different opinions on priorities, directions of urban development and the role and significance of different strategic documents. Differences are also noted in the fact that some of the answers are of a very formal nature and should be considered as "official optimism", while others indicate greater freedom of expression. All of these factors may affect the completeness and validity of statements. Therefore, it is difficult at this stage to objectively state in which cities it is bigger and where there is less potential (primarily social and institutional) for undertaking revitalization activities. On the other hand, it is clear that this potential exists in the interviewed cities, and a reliable approach to completing the questionnaire shows that cities have significant hopes in implementing this project. [1]

Regarding strategic documents and planning, cities consider consistently the most important socio-economic development strategy of the city and the general urban plan. In most cases, cities claim that their institutional capacity is sufficient to undertake local development and urban renewal. Similarly, staff fluctuation is not a significant issue. Although the number and potential of social organizations in different cities are varied, it is clearly visible that they are actively involved in the city life. Another answer, containing the most interesting examples of recent activities by civic organizations, shows that in most of the interviewed cities, social organizations have been entrusted (or even have begun) with major public policy actions, especially in the field of social policy. This will undoubtedly be a good basis for including social organizations in revitalizing activities.

Also, the questionnaires allowed to make a mapping of resources and the development directions of the cities on five pillars: social sphere; infrastructure (including the social one as well); water and green spaces; energy efficiency of the buildings; the life quality in the city. Among the social issues, cities have a special focus on actions related to children and youth. This may be a sign of the desire to stop the younger generation from emigrating. The agreement of the cities in this regard should suggest the need to include this topic at national level.

In the same context, all cities could identify easily the most depraved area in their locality. [1]

Another project activity for increasing the level of cities readiness for revitalization processes are workshops that were organised during October – November 2017 and where participated 2-3 representatives from each city: local public authorities (mostly architects, deputy-mayors,

responsible for attracting investments, etc.) and local civic society (schools, active citizens, local NGOs, etc.). The aim of the workshops were to inform the local representatives on the revitalization concept and process based on the Polish experience, but also on good European practises and lessons learnt. During workshops, local representatives could work on concrete tasks in order to train the social oriented revitalization activities identification. Also, a good impact was the possibility to exchange the local practices among cities and municipalities from Moldova within the organised workshops. In this way, local representatives could get inspired from experience of other Moldavian cities (as show the results of the workshops evaluation by the participants). [2]

2.3. Legal framework on Urban Revitalization in the Republic of Moldova

As was shown above, the owner of the urban revitalization process in the Republic of Moldova at the central level is the Ministry of Agriculture, Regional Development and Environment. Within the mentioned project, the Ministry is developing, with the strategic-conceptual support and advisory from the Polish side, the first note-document entitled "Assumptions of the Urban Revitalization in the Republic of Moldova". The mentioned document will be developed at the next phase in a more comprehensive one: "Guidelines of the Urban Revitalization", that actually will represent a policy document.

The assumptions define the general context of the new concept and process in Moldova. The first draft of the document stipulates that the revitalization comes out from the following cities necessities:

- rehabilitation of the heritage of the historical districts, to facilitate organisation the social-cultural events for population in the region;

- improving life conditions in blocks of flats;

- refurbishment and embellishment of the public space - squares, parks, etc. combined with new social activities for citizens;

- upgrading urban infrastructure - from water, gas and electricity networks to roads and public transport networks; including the soft aspect as well.

These actions are to be part of the regional development policy priorities through specific policies and programs. [3]

Urban revitalization is generally defined as follows: "Bringing urban areas to life with the cooperative effort of municipalities, owners and other stakeholders to improve living conditions, enhance environmental and social climate and strengthen the local economy." According to this definition, urban regeneration has 3 pillars: physical, economic and social. Depending on the situation in the area, we need to refer more or less to the three pillars when developing an urban revitalization program. Also, the "Assumptions" document answer to such questions as: why we need the urban revitalization; what does mean this concept for Moldova. It establishes the short and long term objectives, identifies the stakeholders and their roles and shows which funds can be used for revitalization projects at local level. [3]

The guideline will be large consulted with all stakeholders including cities, civic society, etc.

The main idea is that there will not be concrete indications from the centre level, but the local autonomy should be functioning in order to be able for updating the local development plans and documents from the revitalization perspective. The urban revitalization represents in this context, an exercise for the local autonomy of the cities from the Republic of Moldova.

2.4. Piloting phase on Urban Revitalization projects

The very first actions of urban revitalization in the Republic of Moldova will be organised within the piloting phase of the mentioned above project during the 2018 year. After several trainings and study visits in Poland, the responsible persons from the cities of Moldova, based on the polish inspiration, will design project ideas on urban revitalization process. The call will be public but will refer to the cities involved within the project. As a result will be implemented 5-6 projects of urban revitalization.

The evaluation criteria were discussed and consulted with the participants based on the bottom-up approach. All cities were involved in the consultation process. [20]

Parallel with the piloting phase will be organised the elaboration process of urban revitalization programs of the cities. This process will be facilitated by special selected coachers together with the experts from all 4 Regional Development Agencies from Moldova. This will ensure the sustainability of the revitalization process under the guideline of the Ministry of Agriculture, Regional Development and Environment of Moldova.

Based on the results of the piloting phase, in 2019 will be applied a larger financing scheme for urban revitalization projects involving different donors and stakeholders.

3. Conclusions

Urban revitalization represents a complex and integrated process. It involves different stakeholders and requires a high level of local autonomy in terms of capacities and good management. An important step in urban revitalization process is the identification of the degradable area based on a comprehensive diagnostic/analysis of the local situation. The process supposes a high level of the participatory and civic engagement.

In the Republic of Moldova the first steps of urban revitalization are done within the bilateral project with Poland. The Polish experience is very relevant for Moldavian cities so as these two countries have a lot of similarities in terms of history, economic development and good bilateral relations. The urban revitalization process in Moldova implies 3 parallel processes: national level (guidelines document with the role of regulation); piloting phase (implementation of 5-6 projects in cities); urban revitalization programs (at the local level).

The new technologies are used as communication but also an implementation tool in the urban revitalization process.

4. References

[1] Analysis of questionnaires addressed to cities in the Republic of Moldova and Ministry of Agriculture, Regional Development and Environment of the Republic of Moldova on the conditions for the development of urban revitalization and renewal activities. ”Pojekty miejskie” experts. Warsaw, October 2017.

[2] Analysis of urban regeneration trainings evaluation (October – November 2017, Chisinau, Republic of Moldova).

[3] Assumptions of the Urban Revitalization in the Republic of Moldova (draft document). Ministry of Agriculture, Regional Development and Environment of the Republic of Moldova.

[4] BERNT, M.: Partnerships for Demolition: The Governance of Urban Renewal in East Germany’s Shrinking Cities. International Journal of Urban and Regional Research, Volume 33.3, September 2009.

[5] COUCH, C., FRASER, C., & PERCY, S. (Eds.): Urban regeneration in Europe. Blackwell Science, 2003. 227 p.

[6] FLORIDA, R.: Cities and the creative class. Routledge. New York, 2005. 198 p.

[7] GRANATH, M.: The smart cities – how smart can ‘IT‘ be? Discourses on digitalisation in policy and planning of urban development, Linkoping Studies in Arts and Science No. 693, LiU, Sweden 2016, 226 p.

[8] GREEN, J.: Digital Urban Renewal, OT00037-004, Ovum, 2011. 30 p.

[9] GROBERG, R.P.: Urban Renewal Realistically Reappraised. In: Duke Law Scholarship, CGI.

[10] Integrated Sustainable Urban Development chapter of the European Cohesion Policy 2014-2020, European Commission, 26.03.2014.

[11] KERESZTÉLY, K.: Urban Renewal as a Challenge for European Urban Development in the 21st century, 2016. Available on: ‘cities territories governance’ http://www.citego.org/bdf_fiche-document-532_en.html (visited on March 4, 2018).

[12] Law no. 1777 of 9.10.2015 on Revitalization. Dz.U. 2015 poz. 1777. Kancelaria Seimu, 04.11.2015.

[13] Law no. 764 of 27.12.2001 on administrative-territorial organization of the Republic of Moldova. Official Monitor No. 16, art. 53, 29.01.2002.

[14] LE GALES, P. and HARDING, A.: Villes et Etates en Europe, in V. Wright and S. Cassese. (eds), La restructuration de l’Etat en Europe. La Decouverte, Paris, 1996.

[15] LE GALES, P.: Cities in Contemporary Europe, edited by Arnaldo Bagnasco, Cambridge University Press 2000. 178 p.

[16] National Bureau of Statistic of the Republic of Moldova, www.statistica.md (visited on March 4, 2018).

[17] OSWALT, P. and RIENIETS, T.: Atlas of shrinking cities. Hatje Cantz Publishers, Ostfildern-Ruit, 2006. 160 p.

[18] PRAGERT, G.: Polish-Moldavian Project presentation. Project Coordinator, Department of Assistance Programmes, Ministry of Economic Development of Poland. Chisinau, Republic of Moldova, October 2017.

[19] Starachowice Revitalization web page http://rewitalizacja.starachowice.eu/en/

[20] Study visit in Poland, December 2017, http://www.centruinfo.org/2017/12/11/vizita-de-studiu-in-polonia-revitalizare-urbana/ (visited on December 14, 2017).

[21] Urban Renewal, https://en.wikipedia.org/wiki/Urban_renewal (visited on November 26, 2017).

[22] Urban Revitalization in the United States: Policies and Practices. Final report. United States Urban Revitalization Research Project (USURRP). 25 June 2008. Available at: http://www.columbia.edu/cu/c2arl/pdf_files/USURRP_Phase_I_Final_Report.pdf (visited on November 26, 2017).

[23] VERHAGE, R.: Towards a territorialized approach to urban renewal: A comparison of policies in France and the Netherlands, Journal 'International Planning Studies' Volume 10, 2005 - Issue 2, p. 129-143.

ECDL – A BASIC TOOL FOR SMART CITIES

Ronald Bieber[1]

DOI: 10.24989/ocg.v331.6

Abstract
Digital Transformation is changing our society as a whole. New digital skills are required in order to be able to participate in the daily life and work. The OCG has designed a concept "Education 4.0" which enables digital basic skills to everyone. The ECDL – a longstanding worldwide accepted IT certificate – plays an important role within this concept.

Keywords: *ECDL, digital competences, certificate, digital skills, Education 4.0*

1. Introduction

1.1. Digital competence

Digital competences belong to one of the eight key competences of the European Union which were announced as fundamentals for every individual living in a knowledge based society. The European Commission defines digital competence as a critical and confident usage of information and communication technologies for work, leisure and communication [1]. This is in accordance to OCG initiative outlined in subsection 1.2.

A statistic arising from the Digital Single Market of the European Union [2] shows that 169M people between the age of 16 and 74 within the European Union do not have basic digital skills, i.e.: 44% of the European Union population. In this statistic Austria is placed in the better third of all EU-28 countries, ending up with still one third of its population having no or low digital skills as it is depicted in Figure 1. This number unfortunately has not been improved over the last decade. By a closer view to the Digital Economy and Society Index (DESI) of the European Union, Austria has especially in the field of human capital – which implies the required digital skills to benefit from the digital society - and integration of technologies in public and private sector a good standing. Austria is located in the group of the medium-performance countries, which are doing well in certain areas but still need progress in others.

However, there is a clear call for action since several studies predict that within 2020 nine out of ten jobs require at least basic digital skills knowledge.

[1] OCG Austrian Computer Society, Wollzeile 1, 1010 Vienna Austria, ronald.bieber@ocg.at , www.ocg.at

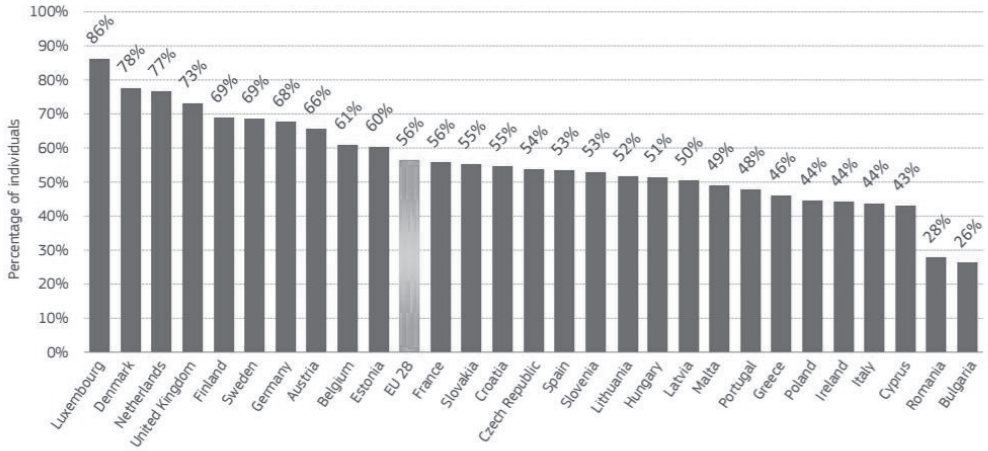

Figure 1: Basic Digital Skills within the EU, 2016, European Commission, Digital Single Market, The Digital Skills Gap in Europe [2]

Digitalization is more and more becoming the driving force today, both in business and in private life [3]. This digital transformation or revolution is after the steam, steel, electricity and petrochemical revolutions, a new change and impulse. The main question is not only what we produce, but also how we produce and how we organize it as a society.

An important driver of the digitalization process is a life long learning attitude among citizens. Hence, earning, updating and reskilling digital skills is one of the main common strategic goals of the government [5]. According Eurostat [6] Austria is on eight place within EU-28 by the percentage of adults doing further education. 14,4% of Austrian people between the age of 25 and 60 are doing further training (EU-28 average reaches only 10,7%). However, there is still a lot additional potential. The leaders, countries like Switzerland and the Nordics, reach values of almost one third of its population doing a separate educational training.

The author of the Digital evolution [5] emphasizes that especially in the educational sector a change of mindset is mandatory. On the one hand digital skills shall already be introduced in primary school sector while on the other hand further education has to be promoted and offered on a low level basis. Besides these actions ICT professional skills have to be established too. Here a clear commitment by the government for a better support in all informatic studies at universities has to be provided. Currently one can study Informatics at eight Austrian universities. Just recently the new Austrian government announced to enhance the number of possible informatic students in Austria by 300 students per year in total.

1.2. Digital competences are a key factor for each economy

A study of the Institute for economic scientific research among Austrian Companies done in 2017 summarizes that about 90% of the companies believe that the current digital transformation ("industry 4.0") is changing their business processes within the next five years. Therefore an increased demand of ICT experts and manpower with digital skills is present. One of the key factors is that the individual is willing for doing further education with respect to digital skills [7].

The more general benchmark which is regularly performed other most European countries and others is the Programme for International Student Assessment (PISA) study of the OECD [8].

This representative study shows that Austria has a remaining gap within the STEM subjects. Figure 2 depicts the development of the last ten years of Austrian students compared with Germany. In all fields Austria has worse results than Germany but even worse the tendency is decreasing in all fields under investigation. In order to have a strong economy one has to have a strong well educated human capital.

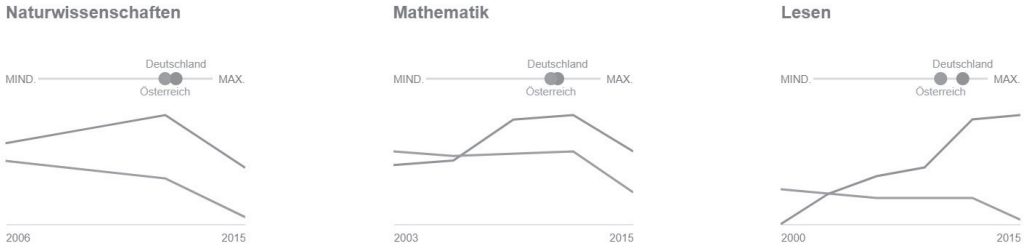

Figure 2: Competences of averaged 15 year old students in STEM (graphic on the left), mathematics (graphic in the middle) and reading (graphic on the right) – results from Germany (blue curve) and Austria (orange curve) [8]

In another special PISA test which is focused on problem solving within a team Austrian students ended up slightly above the average OECD level (score: 509 versus 500). While in the classis PISA tests male students show normally better results than female ones this is the other way round by problem solving tasks. Here the female students had a much higher score than the male (521 versus 498 in Austria).

However, Austria is placed in the middle block of countries and leaves countries like France, UK, Italy or Slovakia behind, the typical leaders are again present, like Singapur (561), Japan (552) or the Nordic countries and also Germany (525).

Due to these facts the Austrian Computer Society started 2016 an initiative in order to enhance digital skills competences within the Austrian population – the so-called Education 4.0 initiative which is outlined in subsection 1.3.

1.3. Education 4.0 – an initiative of the Austrian Computer Society (OCG)

The Austrian Computer Society, a non-profit association for the promotion of information technology with due regard to the interaction with people and society, was founded in 1975 and has currently about 1.400 members out of science, economy and public sector. The association acts as an interdisciplinary forum for the latest IT topics, it is an important and respected dialogue partner and has thematic leadership for socio-political IT topics.

OCG´s initiative "Education 4.0" is based on a three pillar concept which are [9]:

- Computer science, informatics
- Digital literacy and
- Digital media literacy

This concept is similar to the one of the Hasler Stiftung in Switzerland, who developed a new curricula for the german speaking Cantons in Switzerland. The so-called "Lehrplan 21" [10] is now in place and will be implemented in the swiss school system. Media and informatics should become a self standing subject while digital literacy should be implemented within other subjects.

Skills in science, technology, engineering and math (STEM) are becoming an increasingly important part of basic literacy in today´s knowledge economy. Therefore it is essential to be on the forefront of the debate on how to attract more young people to science and technology and how to implement digital literacy in school system. Figure 3 shows OCGs education 4.0 concept at a glance.

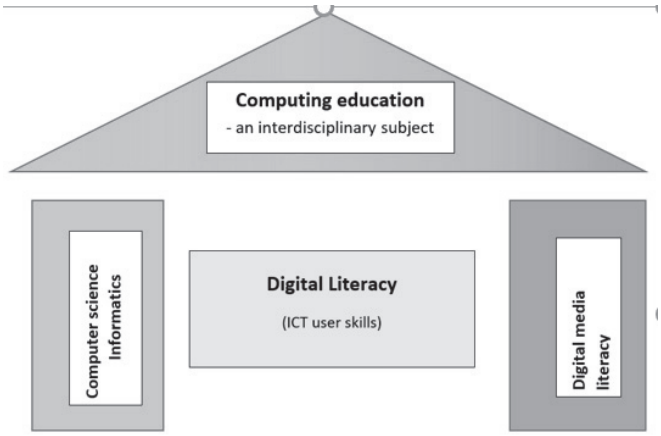

Figure 3: The concept of Education 4.0 – an initiative of the OCG

J. Wing [4] emphasizes that computational thinking is a fundamental skill for everyone. The synonym "computational thinking" was invented around 1980 by Semour Papert, the founder of constructionism. It summarizes basic concepts, tools as well as methods of informatics. It is about looking at a problem in a way that a computer can help us to solve it. This is a two step process: first we think about the steps needed to solve a problem and secondly we use our technical skills to get the computer working on the problem. The focus is towards conceptualizing and not programming. Computational thinking does not necessarily assume experiences on programming but explains concepts and methods of informatics with clarity and depth. Such skills are covered by the first pillar on Education 4.0 "Computer Science, Informatics" and can already be taught in an early stage of education.

The third pillar "Digital Media literacy" means the critical, secure way of how to find and to get information out of internet. Here, OCG is collaborating with several other non-profit associations which have a good network within the school system.

Last but not least, the second pillar "Digital Literacy" means the ICT user skills in general. These skills are mainly covered by the well established European Computer Driving Licence (ECDL), which itself is a success story over the last 20 years in Austria.

The whole initiative "Education 4.0" of the OCG is supported by several well-known associations, like the Swiss Informatic Society, ICT Austria or Digital City Vienna.

1.4. ECDL and its international success

History of ECDL:

The European Computer Driving Licence (ECDL) was founded by a handful European Computer Socities in order to enhance Computer skills in a time when computers were starting to find their way into the working areas. This unique initiative arised from Europe and slowly but continuously it was and is still spreading over the whole world. Currently ECDL/ICDL (International Computer Driving Licence) is established over more than 140 countries in the world. But still 75% of tests are done within Europe but numbers are continuously decreasing compared with the rest of the world – especially in Asia.

One of the first successful implementations of ECDL happened in the Scandinavian countries where a huge number of companies implemented ECDL in their further education of employees. But as soon as every employee has had the certificate no more interest was given. Neither in the school system nor in the unemployed sector the ECDL was established there.

Another development of ECDL happened in Middle Europe. In Italy, UK and also Austria this certificate was soon recognized by Ministery of education and found its way in each particular school system. In Ireland the government soon saw the importance of such a knowledge and introduced it within their public officers as a mandatory certificate.

In absolute numbers only United Kingdom and Italy has up to now more ECDL participants than Austria. Last year Austria was celebrating 20 years anniversary of ECDL and its 500.000 participant. If one looks to the density (number of certificates versus inhabitants) of ECDL diploma holder in each country Austria is ranked in the top four: first place is Malta (it has mandatory ECDL for all school children), second place is Ireland (it has mandatory ECDL for all public officer) and third is Liechtenstein (also established in school system) and on fourth place already Austria is placed. This is due to the outstanding and long established tradition of ECDL in schools and unemployed sector.

The reason for Austrias outstanding numbers are manifold. One important issue certainly is that OCG is heavily involved in several strategic groups of the ECDL foundation, which on the one hand is responsible for operating the ECDL worldwide and on the other hand takes care on new development of modules. Nowadays the ECDL is made for a lifelong learning process. Each participant can and should update her/his skills regularly and can do new modules depending on the needs.

ECDL is a unique product which has overcome more than 20 years in the ICT sector. Over this period the ECDL has performed several changes in the product line. However, one topic remained constant, it is - that ECDL stands for digital skills knowledge.

Structure of ECDL in Austria:

The current ECDL in Austria is clustered in a Base and in a Standard Certificate. The Base consists of four modules namely Computer Essentials, Online Essentials, Word Processing and Spreadsheets. The Standard certificate has seven modules and besides the one of the Base the user can choose three out of five additional modules (presentation, Using Databases, IT Security, Online Collaboration and Image Editing). Besides such standard modules the OCG offers also ECDL Advanced certificates in Word processing, spreadsheets, presentation and Databases, which goes far beyond the common knowledge and shows that the user has professional experiences in using one of these four modules.

This year OCG is planning to install two new ECDL modules: Computing and data protection. The first one is more focused on the school sector while the second one is definitely useful for companies, especially due to the GDPR regulations which will enter into force on 25th of may 2018. Both modules support the approach that ECDL becomes more and more a valid certificate for the workforce and remains a valuable certificate for public and private sector.

The international importance of ECDL is also manifested in the fact that one of the new Board Members of the European Union initiative “Digital Skills and Job Coalition” is the CEO of the ECDL Foundation.

Perception versus reality:

There is a general public opinion that the so-called digital natives (people below 30 years) are more familiar with digital literacy and are not obliged to learn such skills anymore. Therefore several National Operators of the ECDL carried out a digital literacy study in order to determine the real level of digital skills with respect to the perceptions. The studies were done in Switzerland, Denmark, Finland, Germany, India, Singapore and Austria [11] based on similar methods. First participants were asked to self assess their digital skills and second they underwent some practical questions within the requested fields. The results were consistent among the different countries. There was a clear indication that people cannot adequately assess their digital skills. While in Austria 94% of all participants thought to have good or very good general digital skills only 39% ended up with good or very good skills. Singapore – a country always in the top ranking regarding digitalization – shows clearly better results than Austria (55% versus 39%). Nevertheless the self assessment is also far away of the real digital knowledge (88,5% versus 55%) as it is depicted in Figure 4. In all cases the gap between perception and real knowledge increased for the so-called digital natives compared with the older generation.

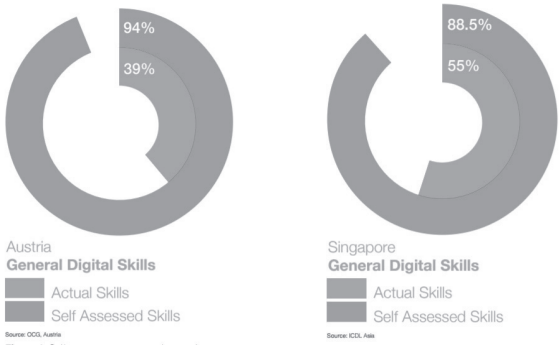

Figure 4: Perception versus reality: General digital skills among Austrian and Singapore population [8].

These results underline the importance of ECDL knowledge also for the younger generation. In Austria the ECDL has also found its way into the public sector. This will be more thoroughly outlined in chapter 2.

2. ECDL within the Austrian public sector

The main two economic sectors currently - where ECDL in Austria is in use - are schools and the unemployed market. Besides this the OCG is looking forward that ECDL is more and more accepted within the public (and also private) sector.

One of the first ECDL public test centers of the OCG was the Ministery of Defence in the beginning of the year 2000. Up to know more than 10.000 officers from the ministery have started the ECDL. Almost half of them have finalized all seven ECDL standard modules.

An even more admirable number are the almost 800 graduated participants who have passed an ECDL Advanced certificate - 113 out of them have even finished all four ECDL Advanced modules and can call themselves an ECDL Expert.

However, on the one hand due to a permanent budget reduction within the Austrian Ministery and on the other hand due to the fallacy of digital natives ICT skills knowledge the ECDL program within the Ministery of Defense has been reduced drastically. So the ECDL unfortunately never got really launched for recruits.

Another Austrian Ministery which counts on the international ECDL certificate is the Ministery of Justice. Several prisons spread over Austria provide ECDL for its prisoners. More than 1000 prisoners have till now successfully passed the ECDL standard – one third of these participants has even obtained an ECDL Advanced certificate. OCG is proud that Austrias biggest youth prison (Josefstadt in Vienna) has been a long standing partner and offers the ECDL for its young prisoners. This is only possible since the public servants who are responsible for the internal process are looking for pragmatic solutions and the OCG has arranged a special agreement with the ECDL Foundation in order to allow tests within prisons. The OCG is still searching for getting the ECDL established within the officers of the Ministery of Justice, too.

Since a couple of years the Administration Academy of the Viennese public officers is cooperating with the OCG in order to enhance its digital skills among their employees. More than 50.000 public officers are working for the Vienna city. A study from the Netherlands [12] came to the conclusion that good digital literacy skills like word processing or spredsheets can finally sum up in a time saving of more than 2% per each working day. If you assume that a common medium enterprize has about 70 office workers sitting most of their time behind the computer you end up with a yearly saving rate of more than 100.000 €. This high amount (more than one Full Time Equivalent) can be saved only due to well educated people who know how to work efficiently on the computer. The Administration Academy of Vienna has just started the program with OCG. In the first year it evaluated the typing skills among their employees. The last year they already started small office tests in order to judge where the gaps are and which actions should be taken into account in the next upcoming phase.

During the last year the Austrian police academy signed a contract where they committed to the ECDL certification for every student of the police academy in Austria. Currently more than 2.000 students are starting every year this school. According to the Ministery of Interior the number of police students should increase continuously the upcoming years.

The head of the police acadamey knows that basic digital skills are preconditions for a digitalized work. The current ECDL is a mixture of digital literacy and basic know how of media competences. Especially basic knowledge as IT Security and data protection are requirements for police further education. Additionally the Ministery committed to the ECDL for the next five years at minimum.

These few examples show on the one hand the importance of digital literacy within the public sector and on the other hand also the possibilities which the ECDL certificate can give for people in the workforce.

3. Midterm goals of the OCG

Smart cities can only exist with smart people who knows how to deal with all the digitalized technologies which should support their life. However, it has to be stated that the public sector has other criteria regarding the economical growth as the private sector. Nevertheless one of the major goals of the OCG is to minimize the digital analphabet among Austrians citizens. As stated in the first chapter currently almost one third of all Austrians have no or low digital skills. This number is too high for being able to compete with the best of the world.

In this sense OCG claims a continuos digital education from primary school up to university level. Starting with gaming in which the children get the first impression of computational thinking. In the lower secondary school digital literacy shall be focussed on, which is mainly covered by the ECDL. Finally the students should come in touch with computing, coding and especially media competences. OCG is still fighting for a mandatory digital acceptance test (or even better an ECDL certificate) for university entry. This was established in Italy for some particular universities. Universities are still searching for new students since companies baits graduated secondary higher school leaver in the IT sector with a high starting salary.

OCG believes that with such an educational concept described in section 1.2 Austria certainly can reduce the leak of ICT experts.

4. Summary and Outlook

Digitalization is the driving force today, both in private life and in business [3]. It is more than just an ICT phenomenon but more a technological trend that has impact on society as a whole.

Therefore OCG has developed together with its experts from science and economy an educational concept for bringing digital skills to everyone (Edcuation 4.0) – a major part for success is the international ECDL certificate which OCG promotes and operates since 20 years. ECDL is a success story in Austria and is becoming a more and more important role within the public sector.

The biggest challenges in order to spread digital knolwedge among citizens are on the one side the fallacy that digital natives have already dgital skills for workforce and on the other side the mistake of numerous stakeholders to believe that basic digital skills are not needed at all anymore or that these skills are anyhow already known.

5. Literature

[1] Recommendations of the European Union (Rec/2006/962/EC) on key competences for life long learning.

[2] Digital Single Market EU https://ec.europa.eu/digital-single-market/en/news/digital-skills-gap-europe

[3] VOGELSANG, M. (2010), Comparison of the Models. In Digitalisation in Open Economies (pp. 141-146), Physica-Verlag HD

[4] WING, J. M. (2006), „Computational Thinking“, Communications of the ACM 49 (3)

[5] Die Digitale Evolution, Policy Brief Nr.34 (05/2017), Kompetenzzentrum „Forschungsschwerpunkt Internationale Wirtschaft“, BMWFW

[6] Eurostat, Participation in education and training (based on EU-LFS)

[7] Studie von dem Industriewissenschaftlichen Institut (IWI) bezüglich Industrie 4.0 (https://www.propak.at/) or (https://news.wko.at/news/oesterreich/PROPAK-4.0---Eine-Branche-im-digitalen-Wandel-PWK855-US-1.html)

[8] OECD, Programme for International Student Assessment http://www.oecd.org/berlin/themen/pisa-studie/

[9] Bildung 4.0, Eine Initiative der Österreichischen Computer Gesellschaft (2016)

[10] Deutschschweizer Erziehungsdirektoren-Konferenz (D-EDK) https://www.lehrplan.ch/

[11] ECDL Foundation, Perception & Reality, Position paper of the ECDL Foundation, http://ecdl.org/ecdl-news?i=3027 (last view: 05.02.2018)

[12] CTRL-ALT-DELETE, Lost productivity due to IT problems and inadequate computer skills in the workplace, Universiteit Twente, Netherlands (2012)

THREE MAJOR CITIES OF BADEN-WÜRTTEMBERG - ARE THEY REALLY SMART CITIES?

Thomas Laue and Birgit Schenk[1]

DOI: 10.24989/ocg.v331.7

Abstract
In this paper we discuss the term Smart City and its components, to design a framework to compare three major municipalities of Baden-Württemberg who declared themselves Smart Cities. The theoretical framework is based on scientific definitions for the different terms related to Smart Cities. To compare the cities we gathered open and public data to guarantee transparency of the evaluation. Hence this is only possible when cities are "smart" so that this method is an indicator itself of a Smart City. We focused on three major cities of Baden-Württemberg who already advertise for being a smart city in comparing different studies.

Keywords: *Smart City, Smart Service, Smart Data, Baden-Württemberg*

1. Introduction

The term „Smart City" and all its linked buzzwords e.g. Smart Services, Smart Data etc. are for many people in public service a vague term and holds a lot of issues. The questions result from the term itself and the necessity to objectively verify, if their own city is already a „Smart City". So the paper provides a framework based on the aspects of the term Smart City which allows to benchmark and assess municipalities.

First of all, we need to clarify the term "Smart City". The development of the «Internet of Things» [1], the intelligent connection of real and virtual objects, led to the foundation of the digital transformation in business and the economy which will leave neither government nor public administration at all levels unaffected. Focusing digitalizing in town and country the term «Smart City» has been established.

Smart Cities are towns which are seeking a way to manage the growing complexity in the use and implementation of intelligent networking information- and communication technology to connect its sub-systems and overcome existing barriers to create a single organic whole. [2] Chourabi et al. [3] describe this as follows: «The new intelligence of cities, […] resides in the increasingly effective combination of digital telecommunication networks (the nerves), ubiquitously embedded intelligence (the brains), sensors and tags (the sensory organs), and software (the knowledge and cognitive competence)».

As well as managing complexity with the concept of Smart Cities it is also implemented to manage the future challenges such as urbanization, use of resources, a rising need for security, changing demographics, etc. which will hit us in the coming years because the smart city concept offers various innovative intelligent solutions and brings value to society. The added value comes with the opportunity to offer so called Smart Services tailored to the customer's needs. E.g. in respect of

[1] University of Public Administration and Finance Ludwigsburg, Germany, schenk@hs-ludwigsburg.de

public administration this implies the possibility to offer smart services for citizens to improve their daily life.

Analyzing two European and three national studies of "Smart Cities" allows us to evaluate, if some of Baden-Württembergs cities are already smart cities according to relevant standards. Therefore the theoretical framework is used to link empirical data of these selected studies which all focus on the same or similar aspects when it comes to the topic of a smart city. We benchmarked only cities whose data are publicly available or already used in public studies. Therefore our methodology in itself guarantees that we focus on smart cities and is an indicator of a smart city itself, because transparency is one of the factors of being smart. Three major cities of Baden-Württemberg offer the needed data and are part of the included studies, so we focused on them: Karlsruhe, Stuttgart, Mannheim.

2. National and European Studies of Smart Cities

Our framework is based on the following studies, which focus on Smart Cities Acitivies and Developments: European Smart Cities of Griffinger et al. [4], Digital Economy and Society Index (DESI) [5], "Morgenstadt-Initiative" of the Fraunhofer Institute of Industrial Engineering IAO [6], the Deloitte Index of Digital Competitiveness of German Municipalities [12], and the Ranking of Cities of Cultures [13].

European Smart Cities

There are many areas in which a town can invest in order to be able to offer smart services to become a smart city. Griffinger et al. [4, p.11] identified six key areas: Smart Economy, Smart People, Smart Governance, Smart Mobility, Smart Environment, Smart Living. To describe a smart city and its six characteristic areas Griffinger et al. [4, p. 12] developed a transparent and hierarchical structure, in which each level is described by the results of the level below. A smart city consists of six characteristic areas, which are described by 31 factors. The 31 factors are defined by 74 indicators, which are used for operationalizing and aggregating the relevant factors. To give an example how it works: 'Smart people' as characteristic is defined through the 7 factors (level of qualification, affinity to lifelong learning, social and ethnic plurality, flexibility, creativity, cosmopolitanism/open-mindedness, participation in public life); for instance, the factor 'affinity to lifelong learning' is then operationalized through the indicators 'Book loans per resident', 'Participation in life-long-learning in %' and 'Participation in language courses'. [7, p. 14]

The ranking approach of 2007 [p.11] focused on medium sized cities in Europe and the following objectives:

"*(1) transparent ranking of a selected group of cities*

(2) elaboration and illustration of specific characteristics and profiles of every city

(3) the encouraging of benchmarking between selected cities

(4) identification of strengths and weaknesses for strategic discussion and policy advice."

Due to accessibility and quality of data 70 European cities were ranked starting in 2007 [4, p. 14, see also 8].

In collaboration with various private and public partners the original Smart City Model was continuously improved considering definitions and data base. At the moment the 4th version is available. Version 1 focused cities of up to 500.000 inhabitants. Version 4 is enlarged and can be used to analyze cities of 300.000 to 1.000.000 inhabitants. Therefore version 4 consists of 27 factors and 90 indicators.

Digital Economy and Society Index (DESI) of the EU[5]

This index focusses on the digital economy and society. It is a composite index that summarizes relevant indicators on Europe's digital performance and tracks the evolution of EU member states and therefore its cities in digital competitiveness. It focusses on five dimensions: connectivity, digital skills, use of internet, integration of digital technology, and digital public services. The five dimensions are described by sub-dimensions containing indicators. E.g. Digital Skills are based on two sub-dimensions (see fig. 1): (a) basic skills and usage and (b) advanced skills and development. [9]

(a) basic skills and usage	Internet users	People who use the internet at least once a week	All people aged 16-74
	at least basic digital skills	Skills such as using a mailbox, editing tools etc.	All people aged 16-74
(b) advanced skills and development	ICT Specialists	Including jobs like ICT service managers, ICT professionals, etc.	Employed people
	STEM graduates	People with a degree in science, technology, maths or engineering-related subjects	All people aged 20-29

Figure 1: Example of the DESI Indicator List

The aggregation of indicators into sub-dimensions, sub-dimensions into dimensions and the dimensions into the overall index uses simple weighted arithmetic averages following the structure of the index e.g. [10, p.20]:

$$(City) = Connectiv(City) * 0.25 + Human\_capital(City) * 0.25 + Use\_of\_Internet(City) * 0.15 + Integration\_of\_Digital\_Technology(City) * 0.2 + Digital\_Public\_Services(City) * 0.15$$

The DESI was developed to have a sound basis for strategy development considering the relevant indicators on Europe's current digital policy mix. The index allows the following main types of analysis [10, p.5]: (a) General performance assessment of individual Member States (b) To pinpoint the areas where Member State performance could be improved. (c) To assess whether there is progress over time and (d) to cluster and compare Member States according to their index scores.

Morgenstadt-Initiative of the Fraunhofer Institute of Industrial Engineering IAO [6]

The Fraunhofer Institute of Industrial Engineering and its partners of industry and Municipalities worked on "smart solutions" to develop a city based on four pillars measured by 28 indicators[2]:

(a) *Quality of life* which means that the city offers jobs, balances between rich and poor, offers attractive surrounding and public space to meet other people, as well as sustainable environment.

[2] For the detailed list of indicators see: https://www.morgenstadt.de/de/loesungen/loesungen_staedte/morgenstadt-index.html

(b) *Resilience* which focuses on stability and preparedness for volatile changes in climate, demographic development, and on the economical basis (Grundlagen)

(c) *Environmental justice* which pinpoints on alternatives of high CO^2 emission within its economy ("CO^2- Ausstieg"), and sustainable resource management

(d) *Innovation* such as encouraging innovation that research institutions and highly qualified employees are attracted by the city. An innovative city offers an "open laboratory" and develops social and technical innovations as well as urban solutions.

The goal of the model was to help municipalities to judge their momentarily situation. Based on the hypothesis that each city is a unique complex system it was not following the idea of benchmarking cities, but to allow each city take a snapshot of their situation to identify a tailored strategy for transforming and developing their city using digitalization. Nevertheless it is possible to use the indicators for a benchmark of cities, because it shows the various urban development processes of municipalities.

Deloitte Index of Digital Competitiveness of German Municipalities [11]

The study focuses on the performance and efficiency of municipalities considering digitalization and the digital age since digitalization is the major factor of being competitive within all branches. Therefore it focuses on the factors which encourage and improve digitalization as well as guarantee companies the needed factors. Three areas are analyzed:

(a) Providing Talents: level and dynamic of employment on the ICT sector, ICT professionals and ICT professions, students in the area of technology, ICT and design, as well as the share of academics of working people.

(b) Encouraging Innovation: number of research institutes, number of ICT companies, number of start-ups in the digital sector.

(c) Attractiveness of location: attractiveness for companies and for students.

The study points out that these three areas are essential for a prospering economy. E.g. qualified workforce helps to increase economy based on technical and social innovations, new business ideas and business models, etc. Networking companies and universities guarantee start-ups a perfect location to develop new ideas. Attractive cities even provide an open-minded atmosphere for different kinds of educated people and international exchange.

Ranking of Cities of Culture [12]

Attractiveness and diversity of a cultural landscape are aspects of quality of life. Therefore people tend to live and work in cities which offer these aspects. If a city wants to attract highly qualified people it has to focus on them. Additionally attractive and diverse cultural landscape improves the image of a city and has a highly stimulating effect on the dynamism of a town and its economy. The consequence is a cultural industry which itself supports economy in the whole and leads to prospering municipalities. One example of a prospering region because of investments in a cultural infrastructure is the Guggenheim Museum of Bilbao, Spain. The index focuses on different aspects

of cultural life in cities such as visiting cultural events (theater performances, cinemas, concerts, as well as even libraries) differentiating between two indicators: production and reception of culture.

3. Consolidated Evaluation Framework of a Smart City and results

Karlsruhe, Stuttgart and Mannheim are three of the cities which were considered in the different studies. Since we wanted to identify the top three smart cities of Baden-Württemberg we selected them considering the following criteria:

(a) population > 150.000 inhabitants

(b) existence of universities

(c) cities which already communicate that they are "smart"

(d) "Schwarmstadt" – with high attractiveness for people aged between 20 and 34

(e) Transport system linked to local, regional, national and international transport – public transport, airports, etc. within 25 km

(f) Cultural facilities such as theatre, museum, etc.

Analyzing the structure and the different levels of structuration throughout the different studies, we noticed that most of the indicators find its pendent cross-reading the studies. So we decided to focus on the areas Smart Economy, Smart Mobility, Smart Environment, Smart Living, Smart Governance and identified seven relevant indicators (see [13], App.B). The weight of each indicator is equal and the assessment of the indicators is based on a scale ranging from 0 to 10 points [13]. So for each indicator a maximum sum of 70 points can be reached within one area.

The following figure shows the results comparing Karlsruhe, Stuttgart, and Mannheim based on the smart areas:

Area	Karlsruhe	Stuttgart	Mannheim	Means
Smart Economy	23	40	23	*29*
Smart Mobility	37	27	27	*30*
Smart Environment	28	23	28	*26*
Smart Living	40	37	29	*35*
Smart Governance	65	55	55	*58*
Sum	193	182	162	*178*
Rank	1	2	3	-

Figure 2: Result of the comparison

Smart Economy

The area of Smart Economy describes the possible increase of economic productivity of a city, if she manages a smart crosslinking of all its stakeholders on the regional as well as the national and international level. Knowledge of the economical regional structure and its composition are the essential key factors to arrange this. Several indicators are considered. E.g. the number of companies which are publicly listed tells us about the attractiveness of the location. The number of part time jobs compared to the number of full time jobs gives an idea about the quality of jobs. The number of part time jobs of qualified employees shows that their potential is not fully used and there might be a lack of competitiveness. Therefore we decided to rate 29 % and more part-time-jobs with 0 points. Highly qualified jobs are indicators for a highly attractive location. Considering the location the Deloitte-Study was used with its two indicators: innovative potential and competitiveness.

Factor	*Indices*
Innovative spirit	Deloitte Innovation Index & Deloitte Index of Attractiveness; Number of patents
Entrepreneurship	Number of Start-ups
Flexibility of labor market	Quota of unemployment; share of part-time jobs; share of highly educated jobs.
International embeddedness	Number of listed companies

Figure 3: Smart Economy – Factors and Indices

Smart Governance

Smart Governance includes a smart public administration as well as smart systems for politicians to decide on policies and politics – such as decision support systems to analyze, to compare and to evaluate areas of policies and politics as well as the impact of decisions. It is also necessary to cope with high complexity and to take citizens along. Major factors are therefore transparent government including Open Data Portals, Online-Participation and an overall strategy for participation.

Factor	*Indices*
Participation	Emergency plans for natural disasters; Non-currant provisions for natural disasters; Strategy to cope with change of climate
Transparent Governance	Open Data Portal; Strategy for participation of citizens; Online-Participation Portal

Figure 4: Smart Governance – Factors and Indices

Smart Environment

Within smart environment we focus on environmental protection, pollution reduction and sustainable resource management. These are factors which can be linked to change of climate. Reduction of garbage and energy saving are reducing resource consumption.

Factor	*Indices*
Environmental protection	Grün- und Wasserflächen im Stadtgebiet
Pollution	Greenhouse Gas Emission; Amount of Garbage
Sustainable resource management	Share of regenerative energy; Smart Grid Projects; recycling of solid waste

Figure 5: Smart Environment – Factors and Indices

Smart Mobility

Smart Mobility describes a city which is working energy-efficient with low emissions, which supports comfortable and reasonable modes of transport while using smart systems for traffic

control. Broadband is the backbone of smart traffic control and therefore is a mandatory precondition.

Factor	*Indices*
Sustainable & innovative transport systems	Situation of cyclists; number of accidents; mobility safety; number of e-stations;
Accessibility	Use of public transport; commuters in % of employed people; number of cyclists
Availability of ICT-Infrastructure	Broadband per household

Figure 6: Smart Mobility – Factors and Indices

Smart Living

Quality of life is the major concern of smart living. So the smart combination of innovative technologies and topics which are relevant for citizens such as Urban Gardening, Smart Home, Smart Health Care as well as cultural programs, education programs etc. are used to increase quality of life. Since the quality of life attracts people and business it is one factor of being competitive.

Factor	*Indices*
Cultural facilities	International rank as a city of culture
Health conditions	Number of hospital beds; Number of doctors;
Individual safety	Number of burglars;
Housing quality	Rental costs;
Education	Quota of students
Social cohesion	Poverty rate and poverty quota

Figure 7: Smart Living – Factors and Indices

4. Discussion and Future Work

Rankings are one tool to focus on important parameters to judge and to compare the performance and the attractiveness of a city considering major areas. The problem of various rankings lies in their basis which differs. “I only believe in statistics that I doctored myself” “The only statistics you can trust are those you falsified yourself," as Winston Churchill once remarked, shows the problem with rankings and studies [14]. Therefore we decided to have a closer look on cities of Baden-Württemberg in existing studies. So we chose these three cities of Baden-Württemberg to find out if they have really potential for developing in a smart city. This decision led to one limiting factor: We could only consider cities which are already part of a study. So maybe we missed to consider cities which might have had potential of being a smart city but which were not considered in the studies because of other reasons.

The next limitation of our work lies in the selection of areas, factors and indices. As soon as we made the decision to select only some of them, we influenced the result. Maybe the result would be more neutral if we had chosen only indicators mentioned in each study, had clustered them to find out about the factors they support and at last assigned them to the smart areas such as Smart Environment, Smart Governance etc.

At last our approach about assessing the different values of the used indicators of the different studies on the scale of 0 to 10 points might have equaled the real impact of the indicators of a smart city.

Nevertheless our work shows that there is smart city potential in Baden-Württemberg. Since managing complexity and future challenges such as urbanization, use of resources, a rising need for security, changing demographics, etc. which will hit us in the coming years the smart city concept offers various innovative intelligent solutions and brings value to society. So hopefully the cities with smart city potential are supported by the country of Baden-Württemberg as well as federal initiatives. Since Baden- Württemberg (and in general Germany) is far behind other countries when it comes to digitalization and e-government, there is still hope that it can manage to catch up using its potential.

5. References

[1] PETROLO, R., LOSCRÌ, V., MITTON N. (2015), p. 1–11

[2] KANTER, R. M.; LITOW, S. S. (2009), p. 2

[3] CHOURABI et al. 2012, p. 2289-2297

[4] GRIFFINGER et al. 2007; http://www.smart-cities.eu/download/smart_cities_final_report.pdf, last accessed 20.02.2018

[5] Digital Economy and Society Index (DESI) 2017, https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2017, 28.02.2018

[6] Fraunhofer Institute of Industrial Engineering: The future of municipalities is digital, https://www.morgenstadt.de/en/news/morgenstadt-werkstatt-2017.html, 23.02.2018

[7] GRIFFINGER, R.; HAINDLMAIER, G.: Smart Cities ranking: an effective instrument for the positioning of cities? Architecture, City, and Environment ACE © AÑO IV No. 12, 02/2010. https://up commons.upc.edu/bitstream/handle/2099/8550/ACE_12_SA_10.pdf, last access 23.02.2018

[8] www.smart-cities.eu, last access 24.02.2018

[9] DESI List of Indicators, https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2017, 24.02.2018.

[10] DESI Methodological note 2017, p. 5, 14.02.2018.

[11] Deloitte – Digital Index 2017/2018 Deutschland, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/deloitte-analytics/DA-DatenlandDeutschland-DigitaleWettbewerbsfaehigkeit-safe.pdf, 26.02.2018

[12] HWWI/Berenberg Kultur-Städteranking, http://www.hwwi.org/fileadmin/hwwi/Publikationen/ Publikationen_ PDFs_2016/2016-09-13_Berenberg_HWWI_Kulturstaedteranking_Studie.pdf , 20.02.2018

[13] LAUE, Michael: Smart City – Baden-Württembergs Städte auf dem Weg in eine digitalisierte Zukunft. Bachelorarbeit, HVF Ludwigsburg 2018.

[14] www.eap-magazin.de, last accessed 20.2.2018

APPENDIX A - Consolidated Areas of Smart City Studies

European Smart Cities	*DESI*	*Morgenstadt*	*Deloitte*	*Cultural ranking*
Smart Economy Innovative spirit Entrepreneurship Economic image & trademark Productivity Felixibility of labour market International embeddedness Ability to transform	Connectivity Fixed Broadband Mobile Broadband Speed Affordability	Quality of life Poverty rate Unemployment rate Rental costs Medical treatment Lebenserwartung der Baby Einbruchsquote Private cars Use of Public Transport Situation of cyclists Air quality Grün- und Wasserflächen	Talent-Index Employment ICT-Sector ICT-Professions Students Share of university graduates	Indicator of cultural production Theatre- and Opera-Seats / 1000 citizens Number of exhibitions / 100.000 citizens Public Libraries: current costs / citizen Denkmalschutz-Fördermittel Cinema-Seats / 1000 citizens Students of public Music Schools per 1000 citizens Quota of employees in cultural companies Concentration of artists / 1000 citizens Zuwendung öffentlicher Mittel für Kulturproduktion
Smart Governance Participation in decision making Public and social services Transparent Governance Political strategies & perspectives	Digital Skills Basic Skills and usage Advanced Skills and Development	Resilient City Share of the 3 biggest companies on employment Independent source of income Dept service ratio	Innovation-Index Research Institutes ICT Companies ICT start-ups	
Smart Environment Attractivity of natural conditions Pollution Environmental protection Sustainable resource management	Integration of Digital Technology Business digitisation e-commerce	Environmental justice Greenhouse Gas Emission Share of regenerative energy Amount of Garbage Water usage Recycling of solid waste	Index of Attractiveness Attractive for companies Attractive for Students	Indicators of Cultural reception Visitors of performances (theatre and opera) / citizens Visitors of museums / citizens User of Public Libraries / 1000 citizens Visitors of festivals / 1000 citizens Sales of cultural companies per citizen Quota of cultural producing companies
Smart People Level of qualification Affinity to life long learning Social and ethnic plurality Flexibility Creativity Cosmopolitanism / Open-mindedness Participation in public life	Digital Public Services e-Government users pre-filled forms online Service Completion Open Data	Innovative City Difference of bankruptcies and start-ups Quota of highly educated jobs Number of patents Quota of students		
Smart Mobility Local accessibility (inter-)national accessibility Availability of ICT-Infrastructure Sustainable, innovative and safe transport systems				
Smart Living Cultural facilities Health conditions Individual safety Housing quality Education facilities Touristic attractivity Social cohesion				

APPENDIX B - Consolidated Assessment Matrix

Area	*Factor*	*Indices*
Smart Economy	Innovative spirit	Deloitte Innovation Index & Deloitte Index of Attractiveness; Number of patents
	Entrepreneurship	Number of Start-ups
	Flexibility of labour market	Quota of unemployment; share of part-time jobs; share of highly educated jobs.
	International embeddedness	Number of listed companies
Smart Governance	Participation	Emergency plans for natural disasters; Non-currant provisions for natural disasters; Strategy to copy with change of climate
	Transparent Governance	Open Data Portal; Strategy for participation of citizens; Online-Participation Portal
Smart Environment	Environmental protection	Grün- und Wasserflächen im Stadtgebiet
	Pollution	Greenhouse Gas Emission; Amount of Garbage
	Sustainable resource management	Share of regenerative energy; Smart Grid Projects; recycling of solid waste
Smart Mobility	Sustainable and innovative transport systems	Situation of cyclists; Number of accidents; mobility safety; number of e-stations;
	accessibility	Use of public transport; commuters in % of employed people; number of cyclists
	Availability of ICT-Infrastructure	Broadband per household
Smart Living	Cultural facilities	International rank as a city of culture
	Health conditions	Number of hospital beds; Number of doctors;
	Individual safety	Number of burglars;
	Housing quality	Rental costs;
	Education	Quota of students
	Social cohesion	Poverty rate and poverty quota

Identity Management

GLOBAL IDENTITY MANAGEMENT FOR INDIVIDUALS? THE RIGHT TO BE FORGOTTEN AND ISSUES OF EXTRATERRITORIALITY

Petra Lea Láncos[1]

DOI: 10.24989/ocg.v331.8

Abstract

The Google Spain ruling of the Court of Justice of the European Union has received much attention (and criticism) both in Europe and the other side of the Atlantic. In this paper I present the decision, focusing on it novel elements and the issues of extraterritoriality. I analyse the problems of extraterritoriality as a function of jurisdiction relying on the presence or absence of links to the EU through the location of establishment, equipment or the target of business activity. Next, I discuss the arguments promoting and rejecting the global application of Rtbf by search engine operators. Finally, I consider extraterritoriality as a practical problem, the solutions offered by scholarship and national courts, as well as their effect on corporations.

1. Introduction

The internet has radically altered the concept of memory – and with it, the public perception of individuals. While the human brain recalls images, sounds etc. in an arbitrary and incomplete way, servers around the world store uploaded data accurately and comprehensively. Yet while the identity of an individual may be reconstructed with the use of data available online, these are all but a snapshot of the diverse life of the person concerned, willing to change and denounce earlier habits or beliefs. Besides relying on the normal workings of human memory, the law has long employed gag orders, anonymity rules, restrictions on access to archives, etc. to promote criminal rehabilitation or to protect privacy. These instruments are rendered more or less ineffective, however, with the perpetual memory of our increasingly digital world.

In its ruling C-131/12 Google v AEPD and González the Court of Justice of the European Union established the right to be forgotten in European Union law, a concept also enshrined in the new General Data Protection Regulation (GDPR). The right to be forgotten seems to be an important legal tool complementing more traditional instruments ensuring accuracy, up-to-dateness, lawfulness and the protection of data. While the right to be forgotten fits seamlessly with European privacy standards, service providers outside the EU are reluctant to adhere to it. In particular, they assert that any request invoking the right to be forgotten beyond European top-level domains is an effort at exerting extraterritorial jurisdiction. Meanwhile, search engine operators resist undertaking new legal, economic and technical obligations.

In the proposed paper I briefly describe the online context of privacy and personality rights violations. Next, I analyse the problems of extraterritoriality as a function of jurisdiction relying on

[1] Researcher, Deutsches Forschungsinstitut für öffentliche Verwaltung, Freiherr-vom-Stein-Str. 2, 67346 Speyer, Germany. Associate Professor, Pázmány Péter Catholic University, Faculty of Law and Political Sciences, Szentkirályi utca 28, 1088 Budapest, Hungary. lancos.petra.lea@jak.ppke.hu.

the presence or absence of links to the EU through the location of establishment and business activity. In particular, I focus on the relevant ruling of the Court of Justice of the European Union (CJEU), revealing the open questions of jurisdiction and the problems of implementing the ruling. Indeed, unresolved issues concerning the extent of search engine operators' obligations and the preliminary reference submitted by the Conseil d'État render this question highly topical. I examine extraterritoriality as a practical problem and consider various solutions proposed in scholarly literature. Finally, I draw some tentative conclusions and raise the issue whether or not the CJEU actually vindicates the authority of global identity management to EU law.

2. Forget-Me-Nots of the Online World

In the analog world, technological advances progressively increased both the speed of spreading news and the accessibility of content on an ever larger scale. News spread by word of mouth, then through newspapers, and eventually, radio and television. Meanwhile, information became a commodity, persons of interest became celebrities and readers and viewers became the consumers in a market where in contrast with backstreet gossip, participants offering and seeking information no longer know each other, with an entire industry built on satisfying the insatiable demand for news. To curb pushy media workers and intrusive paparazzi scraping for crumbs of new information and to restrain editorial rooms keen on landing best-selling headlines, national legislation and regional fundamental rights mechanisms were developed seeking to afford effective protection to private life, personality rights and personal data. Jurisprudence on the protection of public figures and the right to information also evolved.

The digital revolution of the past decades constitutes a new landmark in the evolution of information technology by yet again elevating the spreading and accessibility of information to a higher level. The creation of the world wide web and the availability of multimedia devices was a game changer for the media market, affecting both its structure and actors. Content travels rapidly within our online global village reaching millions, with Web 2.0 websites turning erstwhile consumers into content providers. Media service providers and the advertising sector suffer drastic structural changes, dissipating the traditional *gate keeping* functions of editorial rooms. Information is released unfiltered, spreading unbridled beyond borders and jurisdictions. Anonymity, editing techniques, the speed of spreading information and the multitude of unverified sources lead to the phenomena of 'revenge porn', 'fake news', 'fake porn', etc. calling the credibility of information available online into question. Meanwhile, the „internet doesn't forget":[2] years after publication, information may be easily found and spread online (see [2], p. 84). Every second, a vast amount of data is uploaded to hosting sites, while the content is searchable and may be shared in almost real time. In this context, violations of privacy and personality rights are further exacerbated through the unimpeded spreading of injurious information online (see [4], p. 3).

The shifting technological landscape elicited different solutions from national legislators seeking to meet challenges emerging online and to strike a balance between various fundamental rights, such as the freedom of expression and freedom of information on the one hand, and the respect for

[2] As Marks summarizes: „Since the Google algorithm is not chronologically based, it will be hard for [those concerned] to "escape" their pasts because of the Internet's "inability to forget." (…) If a case that is over a decade old can be revisited in such detail so as to be considered "newsworthy" again and tarnish the image of those who had been able to distance themselves from the events of their past, where is this line drawn? At what point does the Internet's memory begin to intrude upon the protection of one's sense of self? How can one reconcile the American dream of being able to be whoever you want when people can no longer escape their past or change preconceived notions of who they are or what they stand for?" (see [8], p. 42-43).

private life and the protection of personal data on the other (see [18], p. 245; [13], p. 223). At the same time, in the cross-border context of online offences standard questions of private international law may arise regarding the applicable law, the forum having jurisdiction, the territorial scope of the decision taken and even the party liable for implementing the decision. While legislators have been faced with the difficulty of regulating and restricting online activity and arriving at effective solutions for protecting individual rights, this does not mean that legislators could waive their regulatory tasks or the enforcement of privacy and personality rights.

In 2014 the Court of Justice of the European Union breathed new life into Union data protection rules by declaring the right to be forgotten in its *Google Spain* ruling. Against the backdrop of a borderless internet the ruling and the questions surrounding its implementation shed fresh light on extraterritoriality, i.e. the exercise of jurisdiction over activities occurring outside its borders (see [16], p. 227). In the following, I analyse the *Google Spain* ruling to understand the factors the CJEU took into account in order to bring Google Inc. under the *ratione personae* of EU data protection law.

3. Main Findings of the *Google Spain* case

In the instant case, Mario Costeja Gonzales filed a complaint with the Spanish Data Protection Authority in 2009 against La Vanguardia Ediciones SL, Google Spain and Google Inc. Following a *vanity search*, Mr. Costeja Gonzales discovered that the website of the daily publication La Vanguardia featured decade old information on his erstwhile social security debts and auctioning off of his property. Mr. Costeja Gonzales did not deny the veracity of this information, yet he insisted that he had settled his debt years ago and requested that the Spanish Data Protection Authority oblige La Vanguardia to erase or alter the information relating to him and to take action against Google Spain or Google Inc. to remove or conceal the personal data relating to him so that the data no longer appeared in the search results and in the links to La Vanguardia, since these are no longer relevant.[3] The Data Protection Authority upheld the complaint against Google Spain and Google Inc., who in turned challenged the decision before the national court. In the instant case, several question were referred to the CJEU requesting a preliminary ruling.

In its Google Spain ruling[4] the Court of Justice of the European Union declared that under certain conditions, search engine operators are obliged to remove links from the list of results displayed following a search made on the basis of a person's name upon request of the data subject. This right of the data subject enforceable against search engine operators has come to be known as the right to be forgotten. Legislation has since caught up to CJEU case law and the new General Data Protection Regulation of the EU applicable as of 25 May 2018 expressly refers to the right to be forgotten in its Article 17.[5]

The right to be forgotten is not without antecedents (see [11], p. 11; [17], p. 134). indeed, it is the online equivalent of the right to blocking foreseen under the Data Protection Directive.[6] The

[3] Court of Justice of the European Union: Press Release No. 70/14 (Luxembourg, 13 May 2014).
[4] C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD).
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), see further recitals (65) and (66).
[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ *L 281 , 23/11/1995. 0031 – 0050.*

Directive regulates blocking under the title "The data subject's right of access to data" in Article 12 para b) as follows: „Member States shall guarantee every data subject the right to obtain from the controller: (…) as appropriate the rectification, erasure or *blocking* of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."[7] Hence, exercising the right to be forgotten actually means enforcing the right to blocking in an online environment, 'in particular' for reasons of the incomplete or inaccurate nature of the data involved. The latter expression is of great significance, since the applicant in the *Google Spain* ruling did not deny the completeness or accuracy of the data. However, since cases for exercising the right to blocking in Article 12 paragraph b) of the Directive were preceded by the phrase *in particular*, the CJEU arrived at the conclusion that the list in question was not exhaustive. Accordingly, the Court of Justice of the European Union concluded that the right to blocking may be enforced under other circumstances as well. These include situations where the data concerned „are inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary."[8] With this, the CJEU did not necessarily extend, but more precisely defined the scope of cases where the right to be forgotten may be exercised.

The most important contribution of the *Google Spain* ruling is therefore that the Court of Justice of the European Union clarified: EU data protection rules, such as the right to blocking must be implemented in the online context as well (*delisting*). As far as the online context is concerned, the CJEU emphasized that the simple searchability of data makes access to and dissemination of information appreciably easier, which "is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page."[9] This is due to the fact that while sites included in the search results generally published the information concerning the data subject lawfully, collecting such content and making the readily accessible to internet users may magnify the harm caused. Thus, the CJEU separated the individual responsibility of the editor of the website and that of the search engine operator and opened the door to claims made against search engine operators for violation of the data subject's right to privacy. In light of the *Google Spain* ruling of the CJEU, the sole obligor of the right to be forgotten is therefore the search engine operator.

An important finding of the ruling is that the privacy rights of the data subject under Articles 7 and 8 of the Charter of Fundamental Rights „override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having (...) access to the information in question" (see [11], p. 10).[10] The Court of Justice of the European Union clarified that legal recourse is available to the data subjects irrespective of whether the inclusion of the information in the search results causes prejudice to the data subject.[11] This means that delisting requests made by the data subjects do not have to substantiate the occurrence of any specific harm. As a corollary, the search engine operator may only exceptionally deny delisting requests. In case the data concerned is inaccurate, incorrect or no longer relevant, internet users' freedom of information must give way to the data subject's right to privacy (see [19], p. 1122) which, in turn must be enforced by the search engine operator upon request of the data subject concerned. Hence, as a rule, it is the data subject who may decide whether or not information related to him should be readily accessible, albeit only in hindsight. Exceptions, i.e. the denial of a delisting request shall be

[7] Italics by me.
[8] Ruling, para 92.
[9] Ruling, para 87.
[10] Ruling, operative part, para 4.
[11] Ibid.

based on the role played by the data subject in public life and the preponderant interest of the general public in gaining access to the information in question (see [18], p. 250). With this, the CJEU laid down the test to be applied when assessing cases involving the right to be forgotten.

The question, however, arises: on what basis did the Court of Justice of the European Union include Google Inc., a company established in the United States of America, under the scope of European Union law and the jurisdiction of national courts? In the following, I discuss the findings of the CJEU in respect of jurisdiction as well as the relevant question raised in scholarly literature analysing issues of extraterritoriality in the *Google Spain* ruling.

4. Establishing Jurisdiction in *Google Spain*

In its ruling rendered in the *Google Spain* case, the Court of Justice of the European Union declared that search engine operators must be considered 'controllers'[12] within the meaning of the Data Protection Directive, while their activity must be classified as 'processing',[13] since they collect, retrieve, record, organize, store, disclose and make available data in the form of lists of search results.[14] Consequently, activities of search engine operators fall under the scope *ratione materiae* of the Data Protection Directive (see [15], p. 658-659).

The issue of extraterritoriality was raised in relation to the scope *ratione personae* of EU data protection law, the central question being whether a company established in the United States of America, such as Google Inc. may be bound by obligations set forth under Union law. According to the International Law Commission, extraterritoriality is "an attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the State in the absence of such regulation under international law".[15] As Kuner emphasizes, in light of its definition, whether we are speaking of extraterritorial jurisdiction depends on "whether the jurisdictional grounds apply to conduct that takes place outside the State that has enacted it or to parties in another country" (see [7], p. 7). The solution chosen by the CJEU to establish jurisdiction actually calls into question whether we can label it extraterritorial, for although it invokes jurisdiction over conduct outside the EU, it attributes this conduct to a party within its jurisdiction.

Namely, according to the CJEU the link to Union law is established by the fact that data processing is carried out *in the context of the activities* of the Spanish subsidiary of Google Inc., that is the company Google Spain.[16] While the subsidiary Google Spain itself carried out no processing and its activities were limited to the sale of advertising space, the CJEU was satisfied, that establishment of Google Spain in the territory of the EU and the processing activities of Google Inc. create the link necessary to establish jurisdiction. Namely, the Data Protection Directive „does not require the processing of personal data (...) to be carried out 'by' the establishment concerned itself, but only

[12] According to Article 2 para d) of Directive 95/46/EC 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.
[13] Article 2 para b) of Directive 95/46/EC.
[14] Ruling, para 28.
[15] International Law Commission (ILC), "Report on the Work of its Fifty-Eighth Session" (1 May-9 June and 3 July-11 August 2006) UN Doc A/61/10, Annex E, para. 2.
[16] Ruling, paragraphs 52-55.

that it be carried out 'in the context of the activities' of the establishment".[17] In other words, „the activities of the operator of the search engine and those of its establishment situated in the Member State are *inextricably linked* since the activities relating to the advertising space constitute the means of rendering the search engine at issue profitable and that engine is, at the same time, the means enabling those activities to be performed."[18] The inextricable link between the different activities of Google Inc. and Google Spain is further evidenced by the fact that „the very display of [search] results is accompanied, on the same page, by the display of advertising linked to the search terms, [making it] clear that the processing of personal data in question is *carried out in the context* of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory".[19]

An interesting feature of the instant case in Google Spain was therefore that the activities falling under the scope ratione materiae and the territorial scope of EU law were different, including the legal persons carrying these activities, namely the controller on the one hand, and the EU undertaking on the other. However, in order to guarantee effective protection to the data subjects, the Court of Justice of the European Union attempted to piece together jurisdictional links from the facts of the case under the concept of the inextricable *link* of the companies and the activities concerned. As the CJEU elaborated, „the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope."[20] In Scott's assessment, „the EU engages in the practice of *territorial extension* to prompt or provoke different types of legal or behavioural change. (...) Here, the EU is playing the role of a norm catalyst, with the EU measure in question serving to alter the regulatory baseline against which third countries asses the costs and benefits of taking action to address the problem concerned" (see [14], p. 106-108).

Accordingly, the Court of Justice of the European Union seems to rely on the territorial principle when establishing jurisdiction over Google Inc. based on its inextricable link with Google Spain (see [4], p. 8). However, alluding to the principle of effectiveness, the contours of an effects-based jurisdiction may also be discerned. Indeed, according to some scholars Article 4 of the Data Protection Directive establishing jurisdiction is perhaps the most contradictory, misunderstood and enigmatic provision of the Directive (see [3], p. 228). In the course of negotiations on the text of the Directive the concept of processing in the territory of a Member State was gradually broadened, leaning towards a solution based on territorial jurisdiction. At the same time, the Union legislator was aware of the danger that companies may seek to locate their servers in states with more lax data protection regimes, thereby posing the threat of evading jurisdiction based on the territorial principle (escamotage) (see [11], p. 31-32). Therefore, the final text of the Directive related to jurisdiction includes the following wording: „each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State". This broad concept of territorial jurisdiction is coupled with an equally broad understanding of establishment, as evidenced by recital (19) of the Directive's preamble which states that irrespective of the legal form of the undertaking, „establishment on the territory of a Member State implies the effective and real exercise of activity through stale arrangements" (see [15], p. 661). Scott describes this legal construct as follows: „these natural or legal persons may

[17] Ruling, paragraph 52.
[18] Ruling, paragraph 56.
[19] Ruling, paragraph 57.
[20] Ruling, paragraph 54.

either be regarded as being present within the EU or as engaging in EU conduct on the basis that they are offering the services concerned" (see [14], p. 92).

5. The Extent of Delisting Obligations

5.1. Right to be Forgotten: Regional or Global Reach?

According to one point of criticism outlined in scholarly literature, the Google Spain ruling will remain ineffective, since search engine operators will continue to provide unrestricted access to the data concerned 'outside the EU'. In consequence, the protection granted under the right to be forgotten will be rendered illusory (see [18], p. 245). All of this begs the question: what is the extent of the search engine operator's obligation under the right to be forgotten, that is, on which search pages does the search engine operator have to delist the results as requested by the data subject?

As far as the scope of the delisting obligation is concerned, it is worth recalling that in its ruling the Court of Justice of the European Union did not declare that Google Inc. must only delist results covered by the request on national versions of the Google search page. Conversely, it also failed to indicate that the ruling must be implemented globally, on all search pages, including all third country national versions and that with the global web extension .com. This question was left open by the CJEU and was also left unresolved by the GDPR.

The Article 29 Working Party, a consultative body established under the Data Protection Directive, proposed that the delisting be carried out on all relevant pages, including those with the web extension .com. In professional literature this was then interpreted in a way that the Working Party does not suggest global delisting, but merely the enforcement of the right to be forgotten on Member State national versions of the search page and the .com web extension. Following the ruling Google Inc. established an Advisory Council to give guidance on how to fulfil its obligations stemming from the right to be forgotten.[21] The Advisory Council consists of ten members, professionals in the field of data protection, digitalization and information rights, seeking to advise Google on balancing the rights and interests of data subjects and the public at large (see [11], p. 17). The Advisory Council pointed out that 95 percent of all search queries in the Member States are carried out on the national versions of the search pages and not the google.com. That is, internet users do not exploit the opportunities provided by the global search engine (see [17], p. 125).Therefore, the Advisory Council concludes that „in the current state of affairs and technology", removing links from the search results of European versions will provide adequate protection to data subjects (see [11], p. 17). Yet in the current state of affairs it is easily conceivable that the remaining 5 percent of search queries are carried out on the global search page of Google for the very reason that the information sought was not to be found on the national version of the search page, effectively circumventing the restrictions imposed to enforce the right to be forgotten. This would be in stark contrast with the principle of effective legal protection. At this point, the question arises: in case Google Inc., a company established outside the European Union can be included under the scope of Union law, why should the consequences of the enforcement of the right to be forgotten be restricted to the EU national versions of Google?

[21] https://archive.google.com/advisorycouncil/

5.2. CNIL and Global Identity Management

Indeed, this was the position underlying the decision of the French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés (CNIL). One year after the Google Spain ruling and „in the interest of effective legal protection" the CNIL obliged Google in its decision to implement the delisting of results on all of its search pages. According to the CNIL the „decision does not show any willingness on the part of the CNIL to apply French law extraterritorially. It simply requests full observance of European legislation by non-European players offering their services in Europe."[22] Namely, according to the CNIL the Google Spain ruling of the CJEU must be interpreted in a way that delisting requests upheld by the search engine operator must be implemented across all web extensions.[23] Should delisting be limited to only certain extensions, it could easily be circumvented, leading to a hollowing out of the right to be forgotten and the application of different rights to individuals depending on queries of the internet user.[24] The CNIL also pointed out that even a comprehensive delisting affecting all search pages would not amount to a negation of the information rights of the public at large, nor to content censorship, since the content will remain accessible, albeit searchable with different terms and freedom of information will remain under the supervision of CNIL and the national courts.[25]

Google appealed to the Conseil d'État against the decision of the CNIL, arguing that were we to allow the application of one region's law to the entire world, „internet would only be as free as the world's least free place" (see [9]).[26] The extraterritorial application of French (or rather, Union) law is a slippery slope in Google's view, which would be to the detriment of French internet users' information rights and opportunities in the long run. It is important to note that similar concerns were also voiced by academics in scholarly literature – Svantesson goes so far as to envision situations were oppressive dictatorships exploit the opportunity of global delisting to block critical content (see [17], p. 14). Finally, Post raises the question whether the right to be forgotten may lawfully restrict the freedom of expression (see [12], p. 706).

It is important to note that the operation of efficient search engines is a common interest, contributing to asserting individuals' freedom of information. Indeed, search engines may be considered an important element of the communications market, promoting a wide array of fundamental rights directly linked to individuals' information rights. Search engines facilitate access to wide range of political, religious, business, scientific and artistic information underpinning fundamental rights such as freedom thought, political rights, freedom of enterprise, academic and artistic freedom, etc. All this, however, does not mean that search engine businesses would have a legitimate expectation of freedom from regulation: there are legitimate grounds for restricting such activities, including privacy rights of the data subjects. The legislator may thus create the framework for balancing freedom of expression, the interests of the public at large to access information and the individuals' right to privacy and to 'curate their identity' (see [5], p. 1). Regulating search engines' activities indirectly affects the public's right to information and individuals' freedom of expression rendering their assertion less efficient by making restricting easy access to lawfully published data. Therefore, regulatory intervention should not be unduly restrictive. This implies a requirement of proportionality towards the legislator, which may potentially be met should EU decision-makers codify the test devised by the Court of Justice of the

[22] https://www.cnil.fr/fr/node/15814
[23] https://www.cnil.fr/fr/node/15815
[24] https://www.cnil.fr/fr/node/15814
[25] https://www.cnil.fr/fr/node/15814
[26] Peter Fleischer, the data protection advisor's blog post is no longer accessible.

European Union for assessing delisting requests. Legislation should set forth the criteria for screening abusive requests, relying on a delimitation between public figures and information of genuine interest for the public at large, and all other information related to data subjects. Finally, judicial remedy must be available to guarantee an adequate balancing of information and privacy rights, where restrictions are justified and proportionate.

5.3. Conseil d´État paves the way towards legal certainty?

The Conseil d'État proceeding in the case was of the view that it required the clarification of various points of the applicable law and on 21 August 2017 referred several questions to the Court of Justice of the European Union requesting a preliminary ruling. Based on the questions referred, the Conseil d'État is primarily concerned with the extent of Google's delisting obligations under EU law.[27]

With its first two question the Conseil d'État essentially asks whether blocking provisions of the Data Protection Directive[28] prescribe global delisting on all search pages of the search engine operator or only the national version of the Member State where the requesting data subject resides, or all EU national versions, respectively? The third question referred implies a technical solution to prevent the circumvention of blocking: must the right to be forgotten be understood as the obligation of the search engine operator to disable access to the relevant search results by imposing geo-blocking in the Member State where the data subject resides or all EU Member States, respectively (see [1], p. 15)?

This line of inquiry seems to rely on an effects-based approach to jurisdiction which could be an adequate means to assuage extraterritoriality concerns (see [1], p. 12-13). According to the effects-based approach to jurisdiction, any and all activities liable to cause harm in the European Union shall fall under the scope of Union law, or in the present case, under the scope of European data protection law (see [11], p. 26-27; [14], p. 93]. The French Conseil d'État is likely to have been inspired by the *UEJF and LICRA vs Yahoo!* decision, where Yahoo! was sued in France for hosting a site auctioning off Nazi memorabilia. Without directly referring to geographical filtering, the Tribunal de Grande Instance de Paris obliged Yahoo! to take all technically feasible measures to make the site inaccessible in France, stressing at the same time that for the implementation of the decision, web extension-based delisting shall not suffice.[29]

6. Alternative Solutions and Outlook

Those criticizing the right to be forgotten point out that the diverse requirements set forth under the different legal systems impose serious administrative and financial burdens on search engine operators offering services on a global scale. However, in light of the possible privacy and personality rights violations caused by search engine operators, the regulation of such activities is justified. No market operator is entitled to a lack of regulation. Indeed, it is worth mentioning that the provision of other, offline services is also subject to legislative requirements, therefore, legal rules that the service provider must adhere to are a normal corollary of business operations – in this respect, search engine providers are not put at a disadvantage. On the contrary, Tassis and Peristaki

[27] Preliminary reference of the Conseil d'État submitted on 21 August 2017 – Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) (C-507/17) OJ C 347, 16.10.2017, 22–23.
[28] Article 12 para b) and Article 14 para a) of Directive 95/46/EC.
[29] Rg: 00/05308 UEJF and LICRA v Yahoo!

emphasize that the fact that Union law prescribes uniform requirements under the General Data Protection Regulation can much rather be seen as a benefit, since undertakings no longer have to adapt to data protection rules differing from one Member State to the other. As such, the GDPR in fact reduces administrative burdens of undertakings by unifying the data protection law applicable in the Member States (see [18], p. 251). The sheer scale of the European communications market and its elaborate rules on data privacy may even prompt other jurisdictions to copy or converge towards its standards, creating efficiencies also for search engine operators.

Moreover, fears that Google should wind up its subsidiaries established in the European Union have no merit either, since both the effective provision of the Data Protection Directive (Article 4 read together with recital 19) and the provisions of the GDPR entering into force in 2018 (Article 3 read together with recital 22) provide, that irrespective of legal form or the seat of the undertaking, Union data protection law shall be applicable to all processing of the controller where the effective and real exercise of activities through stable arrangements in the Union are fulfilled. Of course, in practice it is difficult to envisage the enforcement of Union law against entities with no subsidiaries established, or servers located in the territory of the Member States.

These difficulties prompted several scholars to propose the regulation of the world wide web as a cross-border phenomenon in an international treaty, where signatory states could jointly regulate the use of the web as well as violations committed online (see [6]; [10]). However, as Ryngaert points out, the feasibility of such an international agreement is more than questionable, given the diversity of regulatory solutions and the balance struck between the fundamental rights of the data subject and the public at large (see [13], p. 223).

By contrast, the Conseil d'État offers the Court of Justice of the European Union an effective and much more feasible solution on a silver platter which could effectively protect privacy and personality rights. Through the application of geo-blocking with effect to the territory of the Member States, the EU could shake accusations of extraterritoriality and global identity management, implementing a technical solution that has been tested and proven worldwide. Geo-blocking would mean that third state and .com web extensions would be spared of implementing delisting requests, while content covered by the delisting request could not be searched from the territory of the Member States by recourse to non-EU search pages. The diverse balance of information rights achieved in other states would remain unaffected, while the effective protection of data subjects in the Union would be guaranteed.

Some criticize the solution referring to the fact that this way, Europeans will know less about themselves and their affairs, than anyone else in the world. However, it is worth pointing out that the test devised by the Court of Justice of the European Union guarantees that only those information be forgotten, the knowledge of which does not breach the rights and interests of the public at large. Thus, timely information of genuine interest to the public, information on public figures and public affairs continue to remain accessible.[30]

Critique is further aimed at the fact that geo-blocking does not provide absolute protection and with the help of certain technical solutions, such blocks may be circumvented. While technically no perfect means exists, this is the solution that from a legal point of view best implements the CJEU's

[30] Cf. Article 29 WP: Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzáles" C-131/12, 14/EN WP 225 (2014.11.26.), 2.

ruling, employing a combination of delisting on EU web extensions and geo-blocking for all other search pages. What may give rise to concern is that geo-blocking can be a means for concealing information from the population and may be used to violate information rights and to manipulate public opinion. Such potential for abuse calls for the devising an elaborate legal background for the use, supervision and technical means of geo-blocking to ensure that restricting access to information complies with constitutional standards. Principles and legal criteria governing the use of geo-blocking in general and in specific cases in particular must be set forth under EU law, including the framework for national controls on the use of geo-blocking. This entails further legislative obligations on both the supranational and the national level to operationalize this new instrument enabling the enforcement of data privacy.

Meanwhile, thanks to the Conseil d'État's request for a preliminary ruling we will soon know more about the extent of search engine operators' obligation under the right to be forgotten and whether the CJEU vindicates the authority to global identity management.

7. References

[1] VAN ALSENOY, B., KOEKKOEK, M., Internet and Jurisdiction after Google Spain: The Extra-territorial Reach of the EU's "Right to be Forgotten", in: Leuven Centre for Global Governance Studies WP. Vol. 152 (2015).

[2] BUCHMANN, J. (ed.), Internet Privacy. Options for Adequate Realization. Acatech study (May 2013).

[3] BYGRAVE, L., Data Privacy Law: An International Perspective. Oxford University Press, Oxford 2014.

[4] FOMPEROSA RIVERO, A., Right to be Forgotten n the European Court of Justice Google Spain Case: The Right Balance of Privacy Right, Procedure, and Extraterritoriality, in: Stanford-Vienna European Union Law WP. Vol. 19 (2017).

[5] GULOTTA, R.− HAAKON, F.−MANKOFF, J., Curation, Provocation, and Digital Identity: Risks and Motivations for Sharing Provocative Images Online, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2012.

[6] DE HERT, P.−PAPAKONSTANTINOU, V., Why the UN should be the world's lead privacy agency (28.04.2016.) https://iapp.org/news/a/why-the-un-should-be-the-worlds-lead-privacy-agency/

[7] KUNER, C., Extraterritoriality and International Data Transfers in EU Data Protection Law. Legal Studies Research Paper Series. No. 49 (2015).

[8] MARKS, D., The Internet Doesn't Forget: Redefining Privacy through an American Right to be Forgotten, in: UCLA Entertainment Law Review. Vol. 23 (2016).

[9] NAUGHTON, J., In the battle of free speech not it's France v Google. The Guardian (09.08.2015.).

[10] MOELLER, C., Respective Roles: Towards an International Treaty for Internet Freedom? http://www.global.asc.upenn.edu/respective-roles-towards-an-international-treaty-for-internet-freedom/

[11] PEROTTI, E., The European Ruling on the Right to Be Forgotten and Its Extra EU Implementation. WAN-IFRA (14.12.2015.) https://ssrn.com/abstract=2703325

[12] POST, R. C., A szólásszabadság amerikai hagyományának magyarázata. Wolters Kluwer, Budapest. 2017.

[13] RYNGAERT, C., Symposium issue on extraterritoriality and EU data protection, in: International Data Privacy Law. Vol. 5 (2015).

[14] SCOTT, J., Extraterritoriality and Territorial Extension in EU Law, in: The American Journal of Comparative Law. Vol. 62 (2014).

[15] STUTE, D. J., Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD, in: Michigan Journal of International Law. Vol. 36 (2015).

[16] SVANTESSON, D. J. B., Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, in: International Data Privacy Law. Vol. 5 (2015).

[17] SVANTESSON, D. J. B., Limitless borderless forgetfulness? Limiting the geographical reach of the 'right to be forgotten', in: Oslo Law Review. Vol. 2 (2015).

[18] TASSIS, S.− PERISTERAKI, M., The Extraterritorial Scope of the „Right to be Forgotten" and how this Affects Obligations of Search Engine Operators Located Outside the EU, in: European Networks Law & Regulation Quarterly. Vol. 3 (2014).

[19] TUTT, A., The revisability principle, in: Hastings Law Journal. Vol. 66 (2005).

THE EFFECT OF THE EIDAS REGULATION ON THE MODEL OF HUNGARIAN PUBLIC ADMINISTRATION

Gábor Klimkó[1], Péter József Kiss and József Károly Kiss[2]

DOI: 10.24989/ocg.v331.9

Abstract

Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market, adopted on 23 July 2014 (hereinafter the eIDAS Regulation) is a significant step towards providing such a predictable regulatory environment that enables secure and seamless electronic interactions between businesses, citizens and public authorities of the members of the European Union. The Regulation ensures that people and businesses are allowed to use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available, moreover, it introduces the concept of trust services and prepares for the harmonization of further areas.

Unfortunately, the eIDAS Regulation together with the Commission Implementing Regulation 2015/1501 is not in perfect harmony with the established and emerging models of operations in public administration in Hungary and consequently a common foundation for secure electronic interaction could be provided only with strong limitations.

To avoid this undesirable situation, the paper proposes the introduction of two registration procedures (built on the basis of the services in the scope of the Regulation) that would complement the missing data items in a transparent manner. This extension would result in the provision of all registered electronic services of the EU countries for all EU citizens.

1. Introduction

The growing internet penetration created a demand for conducting business by on-line means. The private sector responded by offering proper electronic services, and consequently the need for servicing the clients on electronic channels appeared in public administration, too. In order to provide an electronic service to a client there is a need for a proper way of identifying and authenticating the requesting entity (note that in public administration there are different requirements on the electronic identification as opposed to the private sector). The different identification schemes built by the public administrations of separate European countries did not make it possible to offer cross-border electronic identification services. There were studies and pilots to tackle the problem [1], [2], [3]. The final legal solution to deal with the obstacles of cross-border electronic identification services is the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market, adopted on 23 July 2014 (hereinafter the eIDAS Regulation) [4]. The specific measures described in the text of the Regulation, however, are not directly applicable in the model of operations in public administration of Hungary.

[1] Budapest Corvinus University, 1093 Budapest, Fővám tér 13, gabor.klimko@uni-corvinus.hu
[2] MTA Information Technology Foundation, 1525 Budapest Pf. 49., Hungary, mtaita@t-online.hu

1.1. Identification of natural persons in Hungary

In the Hungarian public administration natural persons are identified traditionally by their four "natural" identifying pieces of data, as

- the name of the person;
- the place of birth of the person;
- the date of birth of the person and
- the person's mother's name. [5]

In the case of married women, changing a registered name was usual and accepted therefore a fifth piece of data, the "maiden name" is also used.

Identification in person happens on the basis of a photo ID card (pass) that links the "natural" identifying data with the photo. As computerized registers appeared there was need for using unique identifiers (keys) and for that purpose sectoral identification numbers were introduced (tax identification number, social security number). The official documents that prove the sectoral identification numbers do not have any photo but the natural identifying pieces of data [6]. There were two steps during the in person identification process before processing a sectoral case, as

1. The client was compared to his/her photo on the presented ID card. Having ascertained that the same person has shown the ID card the corresponding natural identifying pieces of data were read from it.

2. The natural identifying pieces of data were compared with the presented sectoral official document. Having stated that they are the same, the sectoral identification number was read.

Note that the set of natural identifying pieces of data is not perfect in the sense that it is not unique; there are a few different existing persons whose aforementioned identifying pieces of data are the same. The Hungarian public administration authorities could live with that shortcoming.

The increased usage of computerized systems naturally led to the idea of using a unified sector independent personal identifier, the personal identification number. This identification number is used in the so-called Register of Citizens that was set up because of Act LXVI of 1992 on Keeping Records on the Personal Data and Address of Citizens [7]. The universal usage of the personal identification number, however, was legally challenged on the basis of constitutional personal data protection principles. The Hungarian Court of Constitution accepted the complaint and in its decision 15/1991. (IV. 13.) declared the usage of a universal personal identification number to be against the Constitution [8].

After the announcement of this decision of the Court of Constitution, only sectoral identification numbers were used while conducting the sectoral cases, otherwise case processing was based on the natural identifying pieces of data [9]. As the "*name of the person*" cannot be considered to be a permanent data item, it was replaced with "*the birth name of the person*". At the end of this process, all the registers that support the operations of the Hungarian public administration provided for natural persons are based on the natural identifying pieces of data. Provision of the natural

identifying pieces of data is compulsory in all administrational processes for natural persons. Registers used in the processes exchange data by using natural identifying pieces of data. The Register of Citizens contains the authentic (trustworthy) personal data, including the natural identifying pieces of data, of persons living in Hungary [7].

In Hungary when a person uses an (on-line) electronic public administration service, he should identify himself by certain means (via the so-called Client Gate [10], [11], or by using an electronic personal ID card). Having been identified the sectoral identification number of the person can be determined on the basis of the so-called *"Disposition Register"* [12]. The raison d'etre of the Disposition Register was the need for such a linking method that is legally acceptable and does not offend the decision of the Court of Constitution. For that purpose, a method based on usage of Encrypted Anonymous Linking Codes (EALCs) was developed, and EALCs of natural persons are stored in the Disposition Register[3]. Storing a new record related to a person into the Disposition Register is done also on the basis of the natural identifying pieces of data. The legal background of this method is laid down in Act XX of 1996 on the Identification Methods Which Replace the Personal Identification Number and on the Usage of Sectoral Identification Numbers [9]. The method is described in detail in [13].

There are, however, such natural persons whose data is not stored in the Register of Citizens but they are entitled to use electronic public administration services by the law. The term "Register of Citizens" refers to two registers, one for Hungarian citizens and another one for such persons that do not possess Hungarian nationality but live permanently in Hungary (they should have a residency permit). Note that the nationality of a client can be determined from these registers.

The need for providing electronic public administration services for foreign individuals, however, was also raised and a dedicated register was set up that contains the data of those foreign clients who want to use electronic Hungarian public administration services. Clients that register voluntarily into this dedicated register are allowed to claim a Client Gate. Note here that owners of the Client Gates also obtain a means of secure electronic delivery of official electronic documents [12].

1.2. Identification of legal persons in Hungary

There are a number of types of legal persons in Hungary. Companies are all legal persons by the Act of V. of 2013 on the Civil Code. Non-governmental organizations can (but are not obliged to) be a legal person, too. There are separate registers for different types of organizations. Affairs of the legal persons are managed and conducted by such natural persons who are entitled (are granted the necessary permission) to do so. Identification of legal persons is therefore referred back to the identification of natural persons.

In order to provide electronic public services for legal persons currently a Client Gate technology (that is bound to a natural person) is used. A new service called "Business Gate" is being offered, however, it can be used only by the authorized (assigned) natural persons, therefore the identification process is based on the identification of natural persons [14].

[3] The homepage of this service can be found at https://rendelkezes.kekkh.gov.hu/rny-public/#en_nav (accessed: 7 March, 2018)

2. The rules of the EIDAS regulation and the Hungarian practice

The EIDAS Regulation enables secure and seamless electronic interactions between businesses, citizens and public authorities of the members of the European Union. The Regulation ensures that people and businesses are allowed to use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available, moreover, it introduces the concept of trust services and prepares for the harmonization of further areas.

However, there are problems with the implementation of the prescripts of the EIDAS Regulation into the Hungarian practice in three areas. We shall scrutinize these areas one by one.

2.1. Identification of a natural person

The Annex of the Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of the eIDAS Regulation prescribes four mandatory and four additional data elements to be transmitted to the affected electronic services. The minimum data set (the mandatory data elements) for a natural person are

(a) current family name(s);

(b) current first name(s);

(c) date of birth and

(d) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time [15].

In the Hungarian practice of operating registers (d) cannot be straight handled as none of the registers is ready to store a unique identifier due to the fact that it is legally forbidden to use such a (unique) identifier for Hungarian citizens. Data element (a), that is, *current family name* is not a piece of permanent data as married women's name often change in a number of countries. As a consequence *the minimum data set is not appropriate for processing a public administration case in Hungary.*

The additional (optional) attributes for a natural person in the eIDAS Implementing Regulation are

(a) first name(s) and family name(s) at birth;

(b) place of birth;

(c) current address and

(d) gender [15].

The (a) *"first name(s) and family name(s) at birth"* is enough for a more specific identification. The (c) *"current address"*, however, is not permanent data therefore it is not appropriate for identification. In order to map to Hungarian practice the "*person's mother's name*" data element is missing. As this data element is compulsory in Hungary, its absence would lead to the modification

of a number of basic Hungarian registers and the related processes. The cost consequences and time requirements of such a change would be highly questionable therefore another solution is needed.

The nationality as a data element is not in the minimum data set for natural persons. There might persons who have eIDAS ID but have no nationality of an EU-member state. For example, Estonia introduced the concept of *"virtual nationality"*, and it is also the case in Hungarian practice that persons with foreign nationality are given the right to use electronic public services. This is problematic from the point of authentication for a cross-border service even when identification is successful. There can be such rights that only citizens of EU countries can be granted and persons of other nationalities are not allowed to have (even when they have a residential permit). In such cases, cross-border services cannot be offered to the identified person. Inclusion of nationality in the minimum data set does not solve finally this problem as nationality is not permanent, but it would improve the current situation.

A particular case in eIDAS identification processes is when the data of a natural person, acting on behalf of another natural person, is to be transmitted [16]. As this data is allowed to be sent without a request and there is no additional attribute with it, it could result in a permanent and comprehensive authorization for all kinds of cases. This approach, however, is not the best solution. In the Hungarian system, one rationale behind the introduction of the Disposition Register was to avoid giving such unconditional authorization.

2.2. Identification of a legal person

The Annex of the eIDAS Implementing Regulation prescribes the following minimal data set for identification of legal persons, too. The mandatory attributes are

(a) current legal name;

(b) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.

The additional attribute are

(a) current address;

(b) VAT registration number;

(c) tax reference number;

(d) the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council (1);

(e) Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) No 1247/2012 (2);

(f) Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013 (3) and

(g) excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012

There is a principle problem with the personification of a legal person. An organization, as an abstract entity, cannot participate in an interactive contact. Rather, a natural person will act on behalf of that organization. It is possible that in the future a robot (chatbot) will act on behalf of the organization but it is meaningless to prepare for this at G2B liaisons. For such purposes a dedicated machine-to-machine connection seems to be appropriate. An example for such a machine-to-machine connection in the Hungarian practice is when cash registers "report" to the tax office, and this communication, of course, differs from human conversation.

According to the EIDAS Implementing Regulation requirement on the minimal data set for legal persons only one unique identifier is to be sent to the affected parties, therefore it is also not a solution if the (representative of the) legal person asks for more than one means for the same identifier. In the Hungarian practice this approach is avoided. If a person acts on behalf of a legal person, the usage of a single identifier (e. g a smartcard) by several persons raises security as well accountability problems; think of the case when a confidential code or the smartcard is passed from one to another. In the Hungarian taxation system, for example, the usage of the Client Gate for electronic VAT reporting is possible for micro enterprises [17]. That led to a situation when the Client Gate of a self-employed entrepreneur was used on behalf of the enterprise by their bookkeeper even though the Client Gate was designed to be a personal tool. The use of a Client Gate by two persons made impossible to determine who was accountable for what in a certain situations.

Any identification method that can be used by more than one individual might cause problematic situations not only for the legal person but for the public administration, too. Let us consider the case of a criminal abuse with legal consequences (e.g. giving an inciting statement), here the electronic identification does not guarantee that the responsible person can be unequivocally identified. However, there is a basic assumption in the Hungarian practice that there is a natural person who wants to act on behalf of the legal person. That is the reason why identification of that person is strictly required and there are separate dispositions that describe the authorizations for different procedures. In summary, organizational level authentication as such is not handled properly.

The eIDAS Implementing Regulation makes it possible in Article 11 (2) the combined verification of data related to a natural person and to a respective legal person [15]. This procedure can be linked (mapped) to the Hungarian practice as it identifies the acting natural person as well as it identifies the represented legal person, too.

Still, there are concerns of this usage. The procedural rights related to a legal person are usually not based on a generic authorization. For example, a bookkeeper might be allowed to represent a legal person only in relation to the Tax Office but in a litigation procedure only the legal advisor of the legal person is entitled to make a statement. Furthermore, it is often the case with transactions of significant value that more than one person jointly are entitled to make a (legal) statement. However, the approach used in the eIDAS Implementing Regulation relies on the concept of having one person's exclusive, unlimited procedural right [15]. Such an unlimited procedural right is usually granted only for the chief executive officer of a legal person.

In the Hungarian practice acting authorizations are recorded in separate registers, for example for tax related procedures authorization data is stored at the Tax Office [18]. For general public

administration matters these authorizations are recorded in the Disposition Register. The administration process is based on the identification of the natural person and on checking his acting authorizations in a separate register. On this basis the combined identification prescribed by the eIDAS Implementation Regulation can be mapped to the Hungarian model of public administration. Unfortunately, this mapping bears significant risks for the legal persons who utilize it as it has been described in the previous paragraph.

2.3. The problem of maintaining contacts

The Regulation ensures that people and businesses are allowed to use their own eIDs to access public services in other EU countries, however, it does not deal with the mutual recognition of the trust services and their possible collaboration. This shortage results in a problem during maintaining relationships with a client.

In the practice of the Hungarian public administration the dominant sequence is the submission of application followed by an administrative decision, where the possibility of a legal remedy for the client is granted by the law. The administrative decision is made by a civil servant who is not always available at the moment of the submission of the application. It is necessary therefore to provide an authentic proof of the time of delivery of the decision to the client, as usually this is the starting time of the deadline of a legal remedy. Had the client refused the receipt of the decision then this will be the starting time of the deadline when the decision becomes final and binding. In order to conduct effective administration it is a basic precondition that the official availability of the client is guaranteed.

The eIDAS Regulation Section 7 introduces the concept of *"electronic registered delivery service*", and its qualified version (*"qualified electronic registered delivery service"*). In Article 44 the eIDAS Regulation also states that "*…the Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data*" [4]. However, the obligation of mutual acceptance among the qualified electronic registered delivery services is not stated. In the world of the paper-based, traditional mail there are international agreements that describes the conditions of the reception and shipping [19]. These issues are not currently addressed by the legal environment for the electronic delivery services.

At this point the interpretation of maintaining (electronic) contacts should be clarified. The eIDAS Implementing Regulation mentions the "*current address"* both for the natural and for the legal persons as part of the minimal data set [15]. The Hungarian practice, however, requires exclusive electronic communication in some areas (for example registering a new company [20], certain tax related administrative activities [17] etc.) for decreasing the cost incurred by the state. In those areas the paper based communication is not possible at all. The duty required for the administrative action harmonizes to the obligation of electronic communication; in a lot of cases the service is free for the client. In these areas, with these conditions the re-introduction of paper-based communication would lead to a disproportionate burden for the Hungarian public administration. The requirement of paying duty for the paper-based version of such services would lead to discrimination for non-Hungarian EU citizens, though it would be based on real excess costs.

In summary, maintaining asymmetric contacts where a foreign citizen submits electronically an application but the Hungarian authorities would be able to respond only in a paper-based manner, is not an acceptable solution. It is necessary to provide a verified delivery for those who identified themselves by an eIDAS-conform identification scheme, too. The ultimate solution would be to

connect the national qualified electronic registered delivery services, but for the time being a temporary solution is to be set up in order to enable the conducting of effective on-line administrative procedures from abroad in Hungary.

3. Proposals for bridging the gap between the EIDAS Regulation and the Hungarian practice

3.1. The case of natural persons

The need for the provision of electronic services already appeared in the Hungarian public administration, in fact it was the reason to set up a separate register for those foreigners who are going to use such services. Limitations that stem from the eIDAS Regulation can be lifted by the development of this register.

We identified three obstacles in the minimal data set for natural persons, as

1) the lack of the name of the mother of the client;

2) the lack of nationality and

3) the lack of the electronic delivery address.

These obstacles could be remedied by using a registration process. Requiring a registration process for the first time when somebody wants to use a Hungarian electronic service by eIDAS identification would not be a substantive burden for the foreign clients. This is a quite a common procedure in webshops or a portal before using the services offered. The current practice is that one could register only by personal appearance into the register of those foreigners who are going to use Hungarian electronic services. It is justified to revise the requirement of personal appearance and let the clients register electronically by using an eIDAS-conform eID scheme, requiring the aforementioned three data elements. The missing data is sent by the identified client who is also allowed to upload scanned documents to support his statements. The upload of supporting documents, however, is not a mandatory condition for the registration as the possibility of submission of false data is low because a client can be identified by his eIDAS-conform eID-service provider. For some types of cases (e.g. land property acquisition) the civil servant could check the uploaded supporting documents and would be able to make a decision. This extension has significance, for example in handling citizenship-related matters as it provides filtering – it is easier to state a false statement than to create a picture of a false document.

Recording of a client into the above mentioned register makes it possible for him to ask for a Hungarian electronic delivery address (and service). As a result, this client has the same possibilities to conduct electronic business with the Hungarian authorities as clients with Hungarian nationality.

3.2. The case of legal persons

A basic obstacle in the mandatory minimal data set for legal persons is that no acting person is referred. The case of the legal persons (organizations) is more complex as currently there is no single Hungarian register for them. The data that describes procedural authorization is stored in a separate register (in the Disposition Register), and they separately register their electronic contact

addresses. These registers are built upon other base registers (the commercial register, register of non-governmental organizations), and, unfortunately, certain types of organizations cannot be properly described. On that basis *it seems justified to set up a new dedicated register for those (non-Hungarian) organizations that intend to use a Hungarian electronic service by eIDAS identification and are not already registered in a related Hungarian register.*

There would be two ways to be recorded into this new register of organizations, as

1) the organization using an eIDAS-conform eID scheme could state who is the authorized person is to conduct business on behalf of that organization. This person could be identified by an eIDAS-conform eID or by a Hungarian identifier; or

2) in case of combined eIDAS identification, where an organization (legal person) and a (natural) person is identified at the same time, the necessary data will be recorded immediately.

The person that was registered with the right of acting on behalf of the registered organization (legal person) could ask for a (qualified) electronic delivery service (address) in a separate step. Having done that, the handling of all legal persons would be routed back to the current Hungarian practice. The person with the acting right whose name is recorded into the new register could give procedural authorization for other persons by entering into the Disposition Register, but now in a selective manner (either related to specific authorities or a specific types of case). That is, that person could take advantage of all opportunities that are guaranteed for Hungarian persons and legal persons.

4. Summary

The rules laid down in the eIDAS Regulation indirectly suppose that there is a unique identifier (both for natural and legal persons) in the different EU countries that is allowed to be used universally for the provision of services. In Hungary, however, the universal usage of a personal identifier is forbidden by the decision of the Court of Constitution. This obstacle can be handled by a registration mechanism on the national level that would be a minimal excess burden but makes effective cross-border usage of electronic services possible.

The Regulation also ignores the requirement of verified electronic accessibility of the client during the administration process (this is the problem of electronic delivery). The ultimate solution for this obstacle is the collaboration of the national qualified electronic registered delivery services. Until this collaboration is implemented, certain national registered delivery services could be extended to maintain contacts with foreign clients.

5. Acknowledgement

This work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016- 00001 titled „Public Service Development Establishing Good Governance” in (the) Ludovika Workshop/Ludovika Research Group/Győző Concha Doctoral Program/Miklós Zrínyi Habilitation Program/István Egyed Postdoctoral Program/Lajos Lőrincz Professor Program.

6. References

[1] LEITOLD, H. (2010) Challenges of eID interoperability: the STORK project. In IFIP PrimeLife International Summer School on Privacy and Identity Management for Life (pp. 144-150). Springer, Berlin, Heidelberg.

[2] MOLNÁR, B., KŐ, A., KISS, J. (2006). Identity-Background Checking a Solution, which Meets the Requirements of Privacy and Personal Data Protection at Identity Management Domain, SEFBIS JOURNAL 1:(1) pp. 22-32.

[3] TAUBER, A, et al. (2010) Towards interoperability: an architecture for pan-European eID-based authentication services. International Conference on Electronic Government and the Information Systems Perspective. Springer, Berlin, Heidelberg.

[4] Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market, adopted on 23 July 2014. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN (accessed: 12 December, 2017)

[5] Act CXL of 2004 on the General Rules of Administrative Proceedings and Services, Available in Hungarian at http://njt.hu/cgi_bin/njt_doc.cgi?docid=85989.328049 (accessed: 12 December, 2017)

[6] PÉTERFALVI, N. et al. Fundamentals of electronic administration, regulated electronic administration services, IT security. Government Window Administrator Postgraduate Education, 5. module. Available in Hungarian at http://kab2.uni-nke.hu/downloads/KAB2_5Modul_1.%20nap_anyaga_elmeleti_resz.pdf (accessed: 1 December, 2017)

[7] Act LXVI of 1992 on Keeping Records on the Personal Data and Address of Citizens. Available in Hungarian at http://www.valasztas.hu/parval2006/en/02/1992_66tv.html (accessed: 12 December, 2017)

[8] HUNGARIAN COURT OF CONSTITUTION, Decision 15/1991. (IV. 13.) 983/B/1990. Hungarian Official Gazette, 1991, No. 39., pp.40.

[9] Act XX of 1996 on the Identification Methods Which Replace the Personal Identification Number and on the Usage of Sectoral Identification Numbers. Available in Hungarian at http://njt.hu/cgi_bin/njt_doc.cgi?docid=26379.344890 (accessed: 12 December, 2017)

[10] EUROPEAN COMMISSION, eGovernment in Hungary, Edition 16.0., 2014. Available at https://joinup.ec.europa.eu/document/egovernment-hungary-april-2014-v160 (accessed: 12 December, 2017)

[11] OECD , OECD e-Government Studies: Hungary 2007, OECD Publishing, Paris (2007). DOI: http://dx.doi.org/10.1787/9789264030527-en

[12] Act CCXXII of 2015 on the General Rules for Electronic Administration and Trust Services, Available in Hungarian at http://njt.hu/cgi_bin/njt_doc.cgi?docid=193173.338642 (accessed: 12 December, 2017)

[13] KISS, J. K., KISS, P. J., & KLIMKÓ, G. (2015) A Model of Secure Interconnection of Registers Containing Personal Data. In Proceedings of the 15th European Conference on eGovernment, ECEG 2015 University of Portsmouth (p. 149).

[14] Government Decree 451/2016. (XII. 19.) on the on the Detailed Rules of Electronic Administrative Services, Available in Hungarian at http://njt.hu/cgi_bin/njt_doc.cgi?docid=199341.346971 (accessed: 12 December, 2017)

[15] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1501&from=EN (accessed: 12 December, 2017)

[16] eIDAS Technical Subgroup, eIDAS SAML Attribute Profile V1.1-2, 2016. Available at: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile (accessed: 12 December, 2017)

[17] Act XCII of 2003 on the Rules of Taxation, Available in Hungarian at http://njt.hu/cgi_bin/njt_doc.cgi?docid=75807.346570 (accessed: 12 December, 2017)

[18] Ministerial Decree NGM 47/2013. (XI. 7.) on the Rules Governing the Electronic Administration of Tax Matters before the State Tax Administration and the Amendment of Other Ministerial Decrees on Taxation. Available in Hungarian at: http://njt.hu/cgi_bin/njt_doc.cgi?docid=164674.287731 (accessed: 12 December, 2017)

[19] Hungarian Post, General Terms and Conditions for Universal Postal Services. Available at: https://www.posta.hu/static/internet/download/PASZF_ASZF01_ASZF_angolul_20131001.pdf (accessed: 12 December, 2017)

[20] Act V of 2006 on Public Company Information, Company Registration and Winding-Up Proceedings, Available in Hungarian at: http://njt.hu/cgi_bin/njt_doc.cgi?docid=101684.339333 (accessed: 12 December, 2017)

RULES FOR EID MANAGEMENT IN THE PUBLIC SECTOR (HUNGARY, 2018)

Alexandra Erzsébet Zámbó[1]

DOI: 10.24989/ocg.v331.10

Abstract

The scope of the bodies providing e-governance services has significantly expanded in the past decade. Electronic identification has become an elementary obligation of the clients in e-procedures, as this is the starting point of any legal electronic transaction.

In Hungary, this legal issue is generally regulated by the Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions, and the related Government Decree 451/2016. (XII. 19.) on the details of electronic administration procedures. These national rules have been adjusted to the provisions of the Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter: eIDAS Regulation).

The aim of the presentation is to summarize the legal possibilities and to evaluate their practical implementation.

1. Electronic ID: gate for e-administration

The electronic identification is a constant topic of discussions about electronic public services, especially because of the frequent transformations of this field. [8] The cause of the latest conversions and the development of the current system is that the European Union has recognized the main obstacle for a digital single market: "a perceived lack of legal certainty makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services." Therefore, the overall control of the electronic identification and trust services has become necessary at the level of an EU regulation. The recent Hungarian legal and organizational framework is the result of the obligatory harmonization of laws and the fulfilment of the targets set by the National Info-communication Strategy 2020.[2] The goals identified in the strategy related to the field of the digital state have been largely fulfilled in the past few years; at least the basic elements have been created. The Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions (hereinafter: E-Administration Act) and the related Government Decree 451/2016 (XII. 19.) on the details of electronic administration (hereinafter: E-Administration Decree) generally regulate the above mentioned field of e-administration.

Whenever we talk about e-governance in the EU, we can bump into the concept of CLBPS (Common List of Basic Public Services), issued in 2001: „Member States have agreed to a common

[1] Assistant Lecturer and PhD Student at the Group of ICT Law, Department of Administrative Law, Faculty of Law, University of Pécs. E-mail:zambo.alexandra@ajk.pte.hu

[2] Nemzeti Infokommunikációs Stratégia 2020, http://www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf [accessed 5 January 2018]

list of 20 basic public services, 12 for citizens and 8 for businesses. Progress in bringing these services online will be measured using a four stage framework: 1 posting of information online; 2 one-way interaction; 3 two-way interaction; and, 4 full online transactions including delivery and payment."[3] The real significance of the electronic ID is linked to the third and fourth levels of the CLBPS list. In the cases of the two-way interaction (third level) and the full online transactions (including delivery and payment – fourth level), the full and authentic identification of the client is inevitable at the very beginning of the legal process. As the E-Administration Act's legal justification says: "The client must identify itself at the point of administration, where the data management makes this necessary. The regulations shall ensure that any of the electronic administration procedures could be done after the use of the electronic identification service."

The aim of this study is to review and summarize electronic identification services granted by public sector bodies, to define the scope of these bodies and other organizations, and I also would like to sum up briefly the main legal provisions affecting clients. Since 1 July 2016, the national regulations have been adjusted to the supranational provisions of the EU. The starting point of this paper is the eIDAS Regulation. In the conclusion, I will evaluate the recent national solutions.

2. The provisions for electronic identification of the eIDAS Regulation

The Recital 12 of the eIDAS Regulation states that one objective is to remove existing barriers to the cross-border use of electronic identification means used in the Member States in order to authenticate, for at least public services. This Regulation does not aim to intervene with regard to electronic identity management systems and related infrastructures established in Member States. The first step towards mutual recognition is to adapt the national identification systems to the conditions specified by the eIDAS Regulation and by the related Commission Implementing Regulations.[4] According to Recital 13 of the eIDAS, Member States have the opportunity (and not the obligation) to notify their electronic identification schemes to the Commission. At least six months prior to this notification, the notifying Member State provides the other Member States a description of that scheme in accordance with the procedural arrangements established by the Commission Implementing Decision (EU) 2015/296 of 24 February 2015. On the other hand, if any Member State notifies the Commission, and this notification is published in the Official Journal of the European Union,[5] all the other Member States shall apply the (mutual) recognition of the notified electronic identification system in their own public procedures where electronic authentication is needed.

It can be stated that the Member States do not strive to ensure interoperability within the shortest possible time, and at present there is little interest in the facilities provided by the eIDAS Regulation, nevertheless, we can assume that all of the electronic identification systems of the Member States fulfil at least the criteria for *low* assurance levels. In Article 8 of the eIDAS Regulation, the electronic identification schemes are classified into 3 assurance levels: "low", "substantial", and/or "high".

---

[3] Communication from the Commission to the Council and the European Parliament - eEurope 2002: Impact and Priorities A communication to the Spring European Council in Stockholm, 23-24 March, 2001 /COM/2001/0140 final/ http://eur-lex.europa.eu/legal-content/HU/TXT/?qid=1520937504379&uri=CELEX:52001DC0140 [accessed 5 January 2018]

[4] Article 7of the eIDAS Regulation and Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015, and Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015.

[5] At present, its is only Germany that uses the opportunity of the eIDAS and has notified the Commission, OJ C 319. (26 of September 2017), p. 3.

The following table shows the most significant differences between each of the security levels:

Security level	Degree of confidence in the claimed or asserted identity of a person is:	Regarding risk of misuse or alteration of the identity, the purpose of the system is:
low	limited	decrease the risk
substantial	substantial	decrease substantially the risk
high	higher than substantial	prevent

It is important to note, that the eIDAS Regulation still remains on the ground of technology neutrality, and it only sets out a minimal number of technical specifications, standards and procedures, taking into account relevant international standards.

Furthermore, the eIDAS Regulation deals with questions of security breaches [Article 10], liability issues [Article 11] and the establishment of an interoperability framework [Article 12], but here I will not go into details as these questions are beyond the focus of this paper.

3. Organizational background of the Hungarian electronic administration

An old-new concept of e-governance has prevailed in Hungary since the E-administration Act came into force on 1 January 2016, for this comprehensive Act deals with every question of electronic procedures, instead of incorporating the rules for electronic administration into several other acts. This Act entirely replaces the previous chapters (II/A. and X.) of the Act CXL of 2004 on the General Rules of Administrative Proceedings and Services. The new code for public administrative law, the Act CL of 2016 on General Public Administration Procedures – which came into force on 1 January 2018 – refers already to the provisions of the E-administration Act when needed as General Rules on Communication [Section 26] and General Rules on the Delivery of Decisions [Section 85]. The legal framework for the *regulated electronic administration services* and for the necessary organizational background is also incorporated into the E-Administration Act.

The electronic administrative processes (within the electronic identification) assume on the one hand the client, and on the other hand the e-governance bodies interaction (or the interaction between the e-governance bodies). Those bodies providing e-governance services can perform their duties if they use *regulated electronic administration services* provided by a specified service provider(s). Electronic identification methods cannot work without authentic state registers in the background. In addition, it seems obvious to set up a supervisory body for the sake of compliance. In this section, I will briefly present the organs participating in the fairly complex process of electronic identification in the course of e-administration procedures.

3.1. Bodies providing e-governance services

According to the E-Administration Act, the bodies providing e-governance services are enumerated in Section 1 Point 17 of this Act.[6] This overall list of 12 points has been barely changed since the

[6] a) government bodies, b) local authorities, c) other legal entities vested with administrative competence by an act or government decree, d) the Országos Bírósági Hivatal (National Office for the Judiciary) and courts, e) the commissioner of fundamental rights, f) the public prosecutor's office, g) notaries public, h) court bailiffs, i) public sector bodies, excluding appellation councils, j) public utility companies, k) legal entities with public service functions

adoption of the Act, although an amendment has been added an explanatory provision that specifies which of the listed bodies are regarded as *public entities required* to provide e-governance services. The bodies listed in the points from a) to k) are legal entities with public service functions or such providing public services. According to a presentation published by the National Info Communication Service Provider Private Limited Company (NISZ), there are approximately 1,2 million bodies in Hungary within the scope of this regulation that are regarded to be *public entities required* to provide e-governance services.[7] [3] These legal entities shall ensure the availability of the means for electronic procedures in accordance with this Act as of 1 January 2018. (In practice, there may occur some difficulties in connection with the execution of this provision for some specific bodies, e.g. public sector bodies, court bailiffs, or local authorities, so we should consider this legal obligation as a developing process.) The merit of this unified list is that in the future, private legal entities – see point l) of the list – can voluntarily join and use the same services, and the same legal requirements shall refer to them as entities providing public services.

3.2. E-governance service providers

The E-Administration Act discusses the *regulated electronic administration services* separately (hereinafter referred to with the Hungarian abbreviation: SZEÜSZ) and the *centralized electronic administration services* (hereinafter referred to with the Hungarian abbreviation: KEÜSZ), although there can be considerable overlaps. The justification of the Act highlights the logic of the regulation, as it declares SZEÜSZ being left open for the private sector, while only state organs can provide the KEÜSZ. In addition to this dual system, another factor complicates the scheme apparently, as the E-Administration Act specifies the SZEÜSZ as services *provided by the Government on a compulsory basis* [Section 34], with services incorporated into the KEÜSZ services.

At present, there is no registered SZEÜSZ service provider in the private sector. KEÜSZ providers – designated by the 84/2012. (IV. 21.) Government decree – are the followings:

a) NISZ National Info Communication Service Provider Private Limited Company (hereinafter referred to as NISZ),

b) IdomSoft Ltd. (a subsidiary of NISZ), and

c) Hungarian Postal Service Private Limited Company.

As a strategically important participant in Hungary, the NISZ has provided telecommunication, IT, and e-government services through its half century long history. Since 2005, the company has been fully state-owned, and the superior body of it is the Ministry of the Interior. According to the provisions of the 84/2012 (IV. 21.) Government Decree, the NISZ activities are based on the public service contract with the minister in charge of e-administration. Some projects of the NISZ (e.g. governmental hotline 1818, unified government file manager) have been carried out as the

---

or providing public services, and required to provide electronic administration services by an act or government decree, and l) legal entities, other than those covered under Paragraphs a)-k), who voluntarily agreed to provide means for electronic transactions under this Act in certain specific cases in compliance with the requirements set out in this Act, and who notifies the Supervisory Authority for Electronic Procedures thereof.

[7]http://www.kormanyhivatal.hu/download/0/0c/04000/Elektronikus%20%C3%BCgyint%C3%A9z%C3%A9s%202018%20janu%C3%A1r%201-t%C5%91l%20_NISZ.pptx. [accessed 3 January 2018]

successor of the previous Central Office of Public Administration and Electronic Public Services (hereinafter referred to with the Hungarian abbreviation: KEKKH) since 1 January 2017.

3.3. The responsible bodies for central registries

After the termination of the KEKKH by succession on 31December 2016, another successor of that central office is the Ministry of Interior, Deputy Undersecretary of State Responsible for the Registers (hereinafter referred to with the Hungarian abbreviation: BM NYHÁT), which is currently the competent authority for the undermentioned registers:

a) the personal data and addresses records,

b) the central address register,

c) cross-referencing register,

d) register of foreign persons relying upon an electronic identification or a trust service,

e) Central Client Registration Database,

f) register for official identification certificates,

and furthermore 12 registers for different purposes.[8] The purpose and the legal basis of data processing are determinative for every register, and it is particularly prevalent for large state registries. The *central immigration register* also plays an important role in the process of electronic identification and it belongs to the authority of the Immigration and Asylum Office.

The abovementioned registries (databases supervised by the state) are essential participants in the process of electronic identification because the authentic information stored in them is a reliable point of reference, in case the e-governance service providers check the identity alleged by a client. The E-administration Act contains some more details about this procedure, which will be mentioned in chapter 4.2.

3.4. Supervisory Authority for Electronic Procedures

The Supervisory Authority for Electronic Procedures (hereinafter "Authority") shall mean a body designated by the Government for facilitating and supervising electronic administration procedures, for the cooperation and coordination of cooperating bodies, and it is tasked to carry out functions delegated in the E-administration Act and the E-administration Decree.[9]

The need for establishing a supervisory authority had emerged earlier than the present solution. There were some ineffectual attempts in 2013 [1], when the legal provisions regarding such authority were put into the Act CXL of 2004 on the General Rules of Administrative Proceedings and Services. The regulations according to the Authority were not only replaced on 1 January 2017 into the chapter IX of the E-administration Act, but the position of this supervisory body was also strengthened and its tasks were expanded.

[8] https://kozigazgatas.magyarorszag.hu/intezmenyek/450021/450094/450285/bmkanvh.html [accessed 5 January 2018]
[9] Section 1. 18., E-administration Act.

The Authority is more than the supervisory body of the SZEÜSZ and the KEÜSZ, it is a central body, as well, having coordinating, advisory, and regulatory powers in respect of the electronic administrative procedures. The Authority has extended inquiry legitimacy and shall order various sanctions.[10] The Authority is also entitled to maintain a database on matters that can be processed by way of electronic means and on bodies providing e-governance services, and shall make this database available to the public.[11] This kind of database can facilitate the orientation of the clients tremendously, and can stimulate the willingness of using electronic public procedures.[12]

4. Basic rules for eID from the perspective of Clients

4.1. E-governance services as rights or obligations

The E-administration Act defines the concept of "client" broadly: "Client shall mean a person or other legal entity involved in matters falling within the powers and competence of a body providing e-governance services in the capacity of a client, party or a subject to the proceedings, or as a relying party or the representative thereof, where such person or other legal entity is not recognized as a body providing e-governance services and is not a member or employee of the competent body providing e-governance services."[13]

From the point of view of a natural person, the client has an enacted *right*[14] to grasp the opportunities of electronic public services, although in some exceptional cases, this right can be limited or even excluded by the act, like in the following cases:

a) an act or government decree adopted in a vested legislative capacity creates an obligation for the physical presence of the client, or for the submission of documents that may not be obtained in any other way,

b) for procedural steps where it is not applicable,

c) for procedures or procedural steps where it is excluded by an international treaty or a directly applicable Community legislation that is binding in its entirety,

d) in the case of any document, official instrument or other petition that contains classified information.

On the other hand, a natural person may be obliged to use electronic administration procedure only by an act.[15] Nowadays it is still a very important legal guarantee because the whole population has not obtained all the ICT competencies and devices needed for e-procedures yet.

---

[10] E-administration Act Section 48.
[11] E-administration Act Section 50.
[12] Unfortunately, at the closing time of the manuscript, there is no such database available on the website of the Authority, only a table about the KEÜSZ services https://euf.gov.hu/eusz-tajekoztatok [accessed 01.05.2018]. Those who are interested can find a lot of information about the electronic public procedures scattered on different websites.
[13] Section 1, 48, E-Administration Act, furthermore, we find some additional interpretative provisions in the Subsections (3)-(4) Section 2.
[14] Subsection (1) Section 8, E-administration Act: "Unless otherwise provided for by an act or government decree adopted in a vested legislative capacity, the client shall be entitled to take procedural actions before the body providing e-governance services electronically, and to make statements also by way of electronic means."
[15] Subsection (3) Section 9, E-Administration Act.

The E-administration Act determines the scope of the clients for whom the electronic communication is *mandatory* in respect of all matters falling within the powers and responsibilities of the bodies providing e-governance services. The list of the obliged clients comes as follows:

a) client economic operators;

b) the legal counsels of clients;

c) the followings when acting as clients:

ca) the State,

cb) municipal governments,

cc) budgetary agencies,

cd) the public prosecutor,

ce) notaries,

cf) public sector bodies,

cg) other administrative authorities not covered in Paragraphs cb)-cf).

Obviously, these are legal persons or their representatives, from whom the legislator can reasonably expect that they obtain the necessary instruments for electronic communication. Beyond the above listed legal persons, the client or his representative is obligated to use electronic administration procedure only where so prescribed by the law, and only if it is applicable to the given matter.

4.2. Obligation of electronic identification

According to the provisions of the E-administration Act Subsection (1) Section 18 "a client shall be entitled to communicate electronically *without electronic identification* if no personal identification data is required for carrying out the same procedural or administrative action or for making the same statement where communication is maintained by means other than electronic." These cases are meant for a rather narrow path, but a typical example for this situation is when the client only wants to ask the administrative bodies for some general information.

In every other case, and that is more typical, the client must identify himself, and as the act declares in electronic administration procedures, the client shall have the option to identify himself:

a) by way of electronic identification service;

b) by way of electronic identification means under Article 6 (1) of the eIDAS Regulation; or

c) by way of electronic identification service provided for in Subsections (3)-(4) Section 18 in the type of procedures and/or in respect of the procedural steps specified in the information published by the body providing e-governance services.

The core elements of the additional criteria referred to in point c) are:

- the client has to take specific procedural actions (registration), where physical presence is required,

- during this procedure it shall be provided to ascertain that the person claiming a particular identity is in fact the person to which that identity was assigned,

- this adequacy is met by a high degree of confidence if the data verified in the process correspond:

a) to that client's natural identification data shown in the personal data and address records, central immigration register, or in the register of foreign persons relying upon an electronic identification or a trust service;

b) to that client's natural identification data shown in the personal data and address records or central immigration register, or to data shown in the register of foreign persons relying upon an electronic identification or a trust service that can be verified directly through the cross-referencing register with a high degree of confidence;

c) to that client's identification data fixed in the administrative disposition; or

d) to that client's personal identification data held in the information systems of the body providing e-governance services, that enables the system to verify the identity claimed by the client by means of identity proofing and verification relying on data held in a public register.

The E-Administration Act Subsection (6) Section 18 offers another kind of opportunity when the client shall be entitled to take specific procedural actions or to make specific statements during electronic procedures if he is able to authenticate himself by means of electronic identification established previously in the client's physical presence. Where such identity provides assurance that the client's name and his other identification data are available, respectively, for the body providing e-governance services and to the electronic identification service provider.

5. The eID services available in Hungary

5.1. eID services provided by law

5.1.1. The electronic identification service

The legal guarantees for electronic identification services, which can be provided by private sector participants as SZEÜSZ, are regulated in the sections 30-33 of the E-Administration Act. In accordance with the regulations examined in the previous heading, it is essential that eID services of any type shall be useable only after a registration procedure, which is based on personal appearance. The Act contains details about the necessary progress of registration and the consequent content of the client registration database.

As the eIDAS Regulation is allowed to be used for public services – the eID management systems grant only "low" security level -, the E-Administration Decree declares that the "low" level security services are also suitable for clients.

5.1.2. Electronic identification services provided by the Government on a compulsory basis

The importance of the electronic identification KEÜSZ[16] is shown by its highlighted place within the regulations of the E-Administration Act, as it has an own heading and the relating Section 35, which has several provisions providing legal guarantees for severe data control and for the prevention of profiling. Based on the Act, clients shall have access to the following electronic identification services provided by the Government on a compulsory basis:

a) electronic identification services provided by way of a personal identification document with storage module;

b) customer port of entry; and

c) partial encoded phone identification.

The Act sets down the steps of the client registration procedure, and it creates the legal basis for the inevitable background database as well, which is called in this case Central Client Registration Database (hereinafter referred to with the Hungarian abbreviation: KÜNY). The tasks and competences according to KÜNY belong to BM NYHÁT.

The exact methods how the client identifying himself with the above listed eID services takes place are specified in the E-Administration Decree as follows:

ad a) through reading the identifying information from the internal storage of the eID card in addition with using a PIN code associated to the eID card,

ad b) through user ID and password,

ad c) through user ID and password (or additional elected secondary authentication factor).

Obviously, the most advanced and secure way of identification of these three methods is using the eID card [7], as it is a multifactor identification method, combining the possession based and the knowledge based proceedings. Since 2016, the new Hungarian personal identity card has had several new functions,[17] the main functions are “ePASS”, “eID”, and “eSign”, which are supported by the internal storage (chip), however, there are few public service procedures still in practice where it can be used. [4]

[16] E*lectronic identification service available to natural person clients* is declared – by Subsection (1) a) Section 34, E-Administration Act – as a regulated electronic administration service, which shall be provided by the Government by way of a designated regulated provider of electronic administration services.
[17] http://www.kekkh.gov.hu/Eszemelyi/in_english [accessed 5 January 2018]

5.1.3. Primary Identification Agency (KAÜ)

The E-Administration Act Chapter VII deals with the so-called KEÜSZ. According to the Act, the Government – by way of a service provider delegated by the relevant legislation – shall provide the *primary identification agency*.[18] This authorized service provider, in particular, the NISZ – previously discussed in heading 3.2. – denominates this service as Central Client Authentication Agent (abbreviated: CCAA, Hungarian abbreviation: KAÜ). (For the sake of clarity, I will be using the abbreviation KAÜ when referring to this kind of KEÜSZ.)

Detailed rules for KAÜ are to be found in the E-Administration Decree Section 127, where the rules make clear that this service is a single point of access to all authentication services recognized by the state, and it shall provide the opportunity for the client to choose from among the accessible eID methods, at least from the followings:

a) all of the electronic identification services provided by the Government on a compulsory basis, (at present these are the 3 services listed in the previous heading 5.1.2.),

b) any electronic identification by SZEÜSZ (just in case any appears in the future provided by private sector participants),

c) eID methods in compliance with the eIDAS Regulation (at present German eIDcard).

As we will see, this is a wider spectrum of possibilities offered by the law than the recent functioning of KAÜ can provide, but we can presume that there is no real need from clients for all of the above-mentioned possibilities yet.

5.2. eID services available in Hungary, 2018

At present, there is just one state-owned service provider granting eID services like KEÜSZ for the bodies providing e-governance services. We can rather think about it as an on-going process, as NISZ informs the clients about its e-public administration services: "The recent years have seen development projects making several e-services available for citizens, enterprises, and public authorities. However, the current range of services is yet to be extended and introduced to users."[19] NISZ has developed digital solutions of identification and authentication, as well as the digital signature, furthermore documents delivery for e-public administration infrastructure. In this paper, I only examine the services related to eID, and not even the digital signature, which is both an identification and a document authentication method.

5.2.1. Citizen's Portal (or customer port of entry, or client gate)

There are three different English phrases for the service available at https://ugyfelkapu.gov.hu/, or https://gate.gov.hu/, respectively. The official translation of the E-Administration Act uses the phrase "customers port of entry", the literature calles it "Client Gate" [4] and NISZ introduce this service on its English website as Citizen's Portal.[20] In this paper, I will be using the Client Gate expression in the followings.

[18] Subsection (1) j) Section 38, E-Administration Act.
[19] http://www.nisz.hu/en/services [accessed 05. 01. 2018]
[20] http://www.nisz.hu/en/services [accessed 05.01.2018]

The Client Gate had been the first e-governance application that spread widely among clients. Despite the fact that it is a one-factor, only knowledge based (and therefore considered to be a "low" security level method) eID system, it had a central role and was legally the favoured option during the third era (2009 to 2012) of electronic public administration. [2]

However, it is still the most popular and easiest way to get in touch with the bodies providing e-governance services. According to the latest statistical data at the end of 2017, more than 3 million registered clients had a Client Gate.[21] According to the NISZ English website information: "For those who login to the Citizen's Portal, some 300 e-services become accessible, the most popular being tax and social insurance declarations, university applications, personal document related services, land registry enquiries, and requests for a Certificate of No Criminal Record." Any natural person can register personally for this service, even online, if they have a Hungarian eID card issued after 1 January 2016.

There have been some important differences in the operation of the Client Gate service since the beginning of this year. One of them is that the Client Gate has to cooperate with KAÜ, as this central portal mediates the eID process by the Client Gate to several e-administration services. Another alteration is that the storage service – connected to every user – has been moved to a new portal, the legal expression for it is "personalized communication platform" (abbreviated in Hungarian: SZÜF).[22] This platform is accessible after (at present double) login with the login name and user ID of the Client Gate, and finally, the client can find its legal documents at the new website at https://tarhely.gov.hu/.

5.2.2. Partial Encoded Phone Identification

The legal ground of this service can also be found in the E-Administration Act, but we can find the details of this service only in the General Terms and Conditions[23] of this service granted by the NISZ. This e-service was introduced in 2017 and the main conditions are unchanged. [4]

It is important to emphasize that this service also requires a registration procedure when a preliminary full identification is carried out in the presence of the client by the correlation of the personal documents displayed by the client and the authenticated data gained form the registries. At the same time, there is no natural identity data stored in the registry of Partial Encoded Phone Identification, during the identification process; an encrypted access code will serve for authentication later on. Just as the Client Gate, this type of eID can also be considered as a "low" level security system because it is also based on a knowledge based method.

5.2.3. Central Client Authentication Agent (KAÜ)

The KAÜ operated by the NISZ is to accomplish in a way that government and market identity services (if they appear later on the scene) shall be handled on equal terms. Until this year February, the KAÜ had only provided the choice between the Client Gate and the Partial Encoded Phone Identification eID methods. As I stated earlier in the heading 5.1.3., the E-Administration Act expects to activate the possibility of electronic identification by eID card as well, as it was planned to be incorporated

[21] The source of the number of registered clients of Client Gate from:
https://segitseg.magyarorszag.hu/segitseg/portal/latogatottsagi_adatok.html [accessed 5 January 2018]
[22] Subsection (1) k) Section 38, E-Administration Act.
[23] http://www.nisz.hu/sites/default/files/altalanos_szerzodesi_feltetelek_0.pdf [accessed 5 January 2018]

from the start of this service. [4] This feasibility became available at last on 31 January 2018.[24] This service was devoted to develop, modernize, and simplify the process of the eID, but it still needs some efforts in order to serve these aims properly, and not only by broadening the optional eID methods, but by strengthening the communication security of the portal as well. [6]

6. Conclusions

Constructing a well-functioning e-administration has not only been started, but to formulate it in a more more optimistic way, we can say that we are on the right path with it. There have been some encouraging achievements that can serve as a good basis for the ongoing developments. First of all, it seems to be a good choice that the principal service provider (NISZ) for the public sector is a state-owned Ltd. which has the financial, technical, and professional background for high quality ICT services. Another good item of news is that the Authority could start its operation on a well-based legal ground.

An old drawback of this issue is, however, that it is still very complicated to ensure a good legal basis for these services and procedures. The relating legal rules are not the easiest reading, not even for researchers, as they have become extremely complex, introducing a lot of new phrases, and sometimes iterative rules deteriorate the structure. The principle of technological neutrality is also a big challenge from the legislators' point of view. As this legal field is intended to regulate big state registries containing a huge amount of personal data, the legislation cannot avoid to deal with questions of data protection and to strictly determine the access rights either. [5]

At the same time, we can say that the recent EU and domestic regulations are a little bit ahead of the practical solutions. Member States shall make efforts in order to fill-in the interoperability framework with content, and e-service providers (like NISZ) have to develop and to extend the current range of services. It would be welcomed if the eID card and the electronic signature could gain a more important role, as these are the most secure methods of electronic communication.

In Hungary, the wide range of bodies providing e-governance services now cover all the fields where e-governance services can be expected. The legal basis has been elaborated in the past few years, from this year on, all the affected bodies must become familiar with these regulations. This progress requires not only instrumental (proper hardware and software utilities) development, but organizational and procedural reformation within the above mentioned bodies as well.

According to the three main eID methods available for citizens provided by the KAÜ, it can be established that the most popular solution is still the Client Gate, regardless the fact that it is still the most vulnerable in terms of security. Since there has not been any significant precedent of abuse in the past years, clients prefer (and also get used to) this easily and quickly usable feasibility. The opportunity of using the new eID card for electronic identification from the security point of view is the best choice, however, it is still unusual and a brand new way for most of the public. Another obstacle for the eID card application to become more common is that the potential users have to gain special devices for operating it.

As regards the clients, there is also lot to be done, particularly in order to improve their ICT competences and their knowledge about the already available options. As we consider this

[24] https://hirlevel.egov.hu/2018/02/04/elerhetove-valt-az-eszemelyi-eszig-kartya-a-kormanyzati-kau-kozponti-azonositasi-ugynok-szolgaltatas-mogott/ [accessed 1 March 2018]

development for the future, I suppose that the most useful way to inform and to prepare the prospect clients is to start educating them on the subject of e-governance as early as in the elementary school.

7. References

[1] CZÉKMANN, Zs. CSEH, G., Elektronikus közszolgáltatások a SZEÜSZ-ök tükrében [Electronic public services in the mirror of SZEÜSZ], Publicationes Universitatis Miskolciensis Sectio Juridica et Politica, Tomus Vol. XXII. 2014 pp. 135-145.

[2] KISS, A., KŐNIG, B., Electronic identification and authorization with focus on public administration in Hungary in: CEE e|Dem and e|Gov Days 2015, Austrian Computer Society 2015.

[3] NÉMETH, Á. M., Elektronikus ügyintézés 2018. január 1-től – kötelezettségek, lehetőségek, tapasztalatok [Electronic transactions from 1 January 2018 – obligations, possibilities, experiences]:http://www.kormanyhivatal.hu/download/0/0c/04000/Elektronikus%20%C3%BCgyint%C3%A9z%C3%A9s%202018%20janu%C3%A1r%201-t%C5%91l%20_NISZ.pptx. [accessed 1 March 2018]

[4] ORBÁN, A., BELÁZ, A., eIdentification – Renewable Regulated Electronic Administration Services in: HANSEN, H., et al. (eds.) CEE e|Dem and e|Gov Days 2017, Austrian Computer Society 2017.

[5] POLYÁK, G. SZŐKE, G. L., Technológiai determinizmus és jogi szabályozás, különös tekintettel az adatvédelmi jog fejlődésére [Technoligical determinism and legislation, in particular the development of Data Protection Law], Pro Publico Bono Vol 1/2015.

[6] SZÁDECZKY, T.: Communication security of e-government services. Hadmérnök Vol. XII. No. 2, 2017.

[7] SZÁDECZKY, T.: Data protection and data security of electronic identification documents. Hadmérnök, Vol. XII. „KÖFOP" Issue 2017.

[8] VESZPRÉMI, B: Személyazonosítás az elektronikus közigazgatásban [Identification in electronic administration]. Infokommunikáció és Jog, 2009/34.

eGovernment II

SEMANTIC RECONCILIATION BETWEEN TWO DIFFERENT ASPECTS OF LAW

Bálint Molnár

DOI: 10.24989/ocg.v331.11

Abstract

This paper presents a proposal for reconciliation between the warehouse of legal documents created during legislation and Knowledge Warehouse that is dedicated to assisting both citizens and public officers in the procedural legal rules of Public Administration in Hungary. The Knowledge Warehouse contains several thousand detailed rules that describe how to manage and handle life events of citizens. This description can be considered as generic legal cases within legal procedures of authorities. The citizens trigger specific instances of the generic ones. The evolving Knowledge Warehouse main purpose is to enable citizens to get their specific legal cases started either through Web on the Government Portal or with the help of public officers. The Knowledge Warehouse will be extended by ontologies and semantic search capabilities. An Integrated System for Supporting of Codification will be created in an on-going project that will serve as sound basis for the National Warehouse of Legal Rules. The National Warehouse pursues the prescription of MetaLex legal standards in the case of representation of electronic legal documents. The two Warehouse are strongly coupled to each other. However, the syntactic and semantic structure of both differs profoundly. The representation of e-documents within the National Warehouse is in line with ELI, the European Legislation Identifier, even the ontologies and attached semantic description concentrates on the legal documents structural elements and their interpretation. The Knowledge Warehouse focuses on ontologies of life events and procedures of authorities to leverage semantic searching. The proposed solution tries to reconcile and integrate the two differing approaches.

1. Introduction

Within Public Administration, the *procedural knowledge* for execution and interpretation of legal rules plays key role in relationship with citizens. The goal of this research is to analyze and outline an approach for connecting the representation of the codified and officially published legal rules and the representation of procedural knowledge at both syntax and semantic level. The building blocks of the proposal are the XML schemas and ontologies that enable for carrying out schema and pattern matching.

The formalization and representation of *procedural knowledge* of activities within public administration in XML and relational schema format is the basis. The meta-data related to the codified legal rules following European Union standard [7] serves as a dynamic connector to keep up-to-date the legal rule base for public officers, and ontology that follow a metaphor of citizens' life-events assists the public officers in searching of specific cases and helping citizens. The aim of our proposal is that to formalize the concepts of *procedural knowledge* and *life-events*, to map the syntax level representation of codified legal rules in XML and XML schema onto the sections of the description of procedural knowledge that contain the references and partial, relevant texts of codified legal rules.

To realize the above outlined programme, different models are needed.

1. A concept of *generic document* for describing the procedural knowledge that can be captured through a schema description, and The XML Schema can be considered as meta-data structure of instances of generic documents [12]. This generic document structure provides the opportunity to build a bridge between the syntactical representation of *procedural knowledge* and the representation of *codified legal rules*.

2. The XML structure of generic documents provide the opportunity to connect semantic annotation to certain elements or attributes of documents, the semantic annotation makes use of the ontologies of life events and legal concepts.

3. A *domain ontology* for legal concepts involved in public administration is necessary. In the case of citizens' relationship management, the legal concepts belong to the domain ontology that is dedicated to primarily to public administration, i.e. interpretation and execution of laws related to life events of citizens.

4. A *definite part* of the general *legal core ontology* that model the abstract legal notion and organization of government and judicial system, the concepts included in this part is required to describe the processes of public administration.

5. A model of support system for semantic searching that aids public officers in seeking, locating and providing information in the framework of knowledge management.

The paper presents the XML syntax of the metadata for processes of public administration, describes the core and legal domain ontologies and finally introduces the semantic search system. The proposal is for the creating a reliable, and maintainable link between the *Knowledge Warehouse* and *Integrated Legislative System* (*ILS*) in Hungary.

2. Literature Review

In the past decades, the researches on electronic legal and other document-centric systems have progressed immensely. The documents that describe resources and procedures for legal activities and public administration are represented in dialects of XML [1][2][3]. The Metalex/CEN [5], is a de facto standard in EU Member States and de jure standard in EU Institutions to create legal resources in XML format including the various levels of legislations within an EU Member State. Akomo Ntoso standard was created for legal resources of parliamentary legislation processes and documents generated in judiciary processes [16], the objective of Australian Judgment XML standard was similar [15], moreover there was an OASIS initiative 0. Eunomos [4] contains a legal ontology that allows for legislation-specific and generic definition to cohabitate. The EXTRELLA project [8] makes use of Metalex/CEN standard for defining XML Schema of the Legal Resources [7], LKIF-core describe the legal concepts in OWL [10], LKIF-rules formulate the model of ruled for the legal knowledge. The *Legal Knowledge Format* (*LKIF*) and the *Core Ontology of Basic Legal Concepts* were European Framework projects [9] and the aim of these projects was to provide the opportunity the conversion and mutual mapping between legal knowledge-bases that were created by disparate representation methods of knowledge bases; the projects tried to specify a common knowledge representation for the legal domain that may operate as a nucleus among the diverse approaches of knowledge representation. Ontology for public Administration and Life Events was depicted as an outline proposal in Ref. [14]. OntoGov project [1] created a meta-ontology for e-Government. Some solution even made possible that the structure of precedents and of different interpretations can be marked up within the XML document.

2.1. Syntactical and semantical Reconciliation between two Branches of Legal Domains

There is a network of Government One-Stop Shops in Hungary that provides public administration services for citizens. *Knowledge Warehouse* is a service that is currently available, and contains the descriptions of issues and cases that belong to the responsibilities of public authorities to deal with them. The public officers of citizens' relationship management in One-Stop-Government-Shops use Knowledge Warehouse on a daily basis. Furthermore, the citizens, clients can access the content of Knowledge Warehouse through a Web interface, at least partially, i.e. they can retrieve documents, official forms that are required to initiate a case and a process of public administration, moreover content of general information to be known.

The changing and evolving requirements against the citizens relationship management on the side of clients made necessary the development of Knowledge Warehouse. The progress of technology and the objectives of process improvement of public administration towards a unified and uniform treatment of citizens made possible a refurbishing project for Knowledge Warehouse. The upgraded Knowledge Warehouse offers extended areas of case descriptions, as e.g. on the collection of taxes, levies, customs, excises and other obligations towards the state, furthermore municipal responsibilities, judicial and other public service functions, in addition to the existing administrative cases. Each area of cases has a legal entity who is responsible for uploading and maintaining the case descriptions. Knowledge Warehouse as a complex Information System supports the creation of new case descriptions, building up the connections to the legal resources being in force in order to keep the references up-to-date and to safeguard the compliance between the case descriptions and the actual legal resources. The Knowledge Warehouse has three user target groups: clients, service staff of citizen relationship management who works in different contact forms as personal, telephone and chat customer services, moreover colleagues who work in the back-office. Citizens can access the services and content of the Knowledge Warehouse through an online interface. The public officers of personal, telephone, chat citizen services, and in the back-office who are not directly contacted by clients / citizens may need such information that dedicated to administrative processes and not for use of citizens so that the Knowledge Warehouse should ensure the separation of content on the basis of the need-to-know.

The content of Knowledge Warehouse can be accessed through an on-line interface by citizens. The services of Knowledge Warehouse allow for linking the case descriptions and the relevant official forms, moreover the applications that support the filling-in and submitting of forms to initiate the related process of public administration can be assigned to the related case descriptions. This solution makes possible for a citizen who may search for a specific case and then finding the relevant information and official forms that he or she may continue the fulfillment of forms directly. Several years ago, there was an attempt to support both public officers and citizens in the details of particular processes within public administration through a Web interface in the form of **Knowledge Warehouse** (procedures and routines of public administration processes for managing life events of citizens). Behind the Web interface, there was a set of spread-sheets that contained the meticulous description of routines and the relevant legal sources. It is self-evident, that this solution was neither end-user-friendly nor efficient, thereby the necessary next step is to transform the structure of spreadsheets into conceptual model, i.e. an Entity-Relationship model (Figure 1.) and relational schemas then an adequate database model should be looked for, as e.g. document, graph, column-oriented database etc. solution.

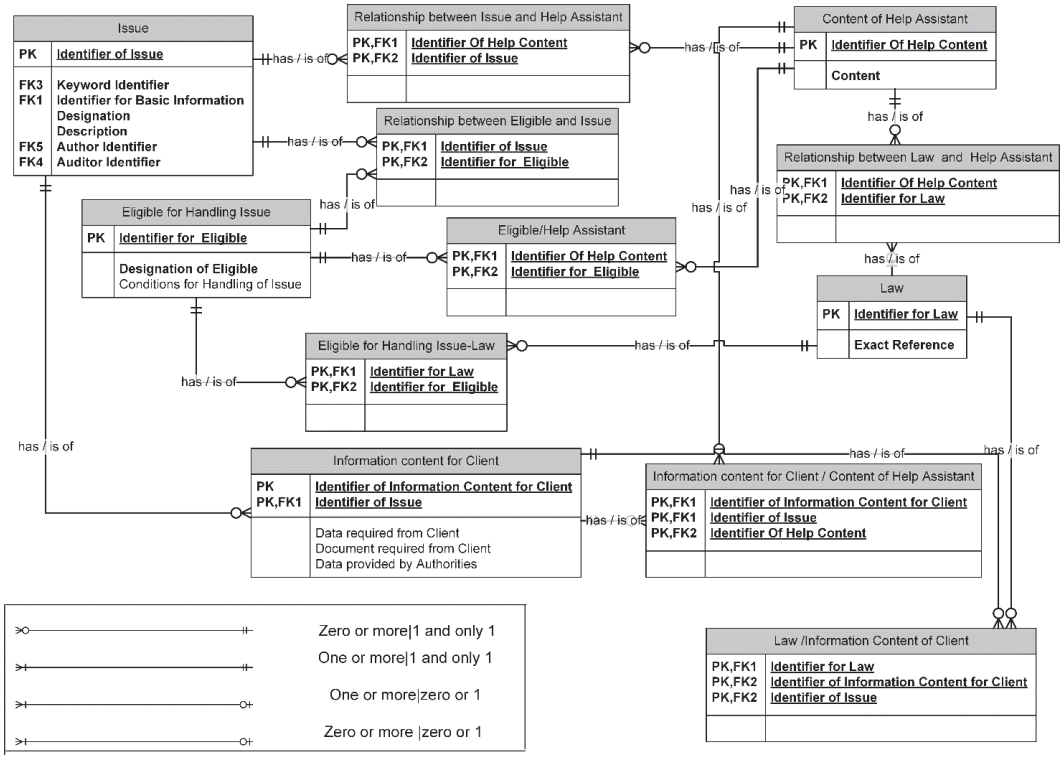

Figure 1: Entity-Relationship Model for Representation of Issues Depicted in Semi-structured Spreadsheets

The core content of Knowledge Warehouse is the database of case descriptions. Case descriptions are based on a generic document type and the instances as the extensions of the generic template are stored in the database. The graph structure of the database represents the mutual relationships among case descriptions, furthermore the connections to legal resources, the links to ontologies, references to templates of documents, forms, and to applications for filling-in forms. The graph structure permits that many-to-many and one-to-many relationships can be represented and the amendments in legal resources can be tracked easily to maintain the timeliness of legal resources.

The case descriptions of the database are linked to the legal resources contained in the *Integrated Legislative System* (*ILS*) and to the official forms that are required to initiate the process of public administration and these forms are stored in the *Unified Central Electronic Document Management System (UCEDMS)*. The *ILS* connection ensures that the legal resources and regulations that are required for the processing of individual cases are available to citizens or public officers in the form and content of the *National Legislation Register* (*NLR*). The *ILS*, *NLR* will use the *European Legislation Identifier* (*ELI*) for the Hungarian legal resources to be used for the clear identification of laws and other legal instruments of public administration. This reference system makes it possible to refer to the syntactical elements of the legislative structure (legal identification, part, chapter, section (§), paragraph, list, etc.) with the necessary detail. When the legal background of a case description is retrieved, the relevant parts of the case description template are highlighted; furthermore, the legal resources in force on the date that is set and selected by the user is also displayed.

The *ILS* connection ensures that the administrators of Knowledge Warehouse will obtain immediate notifications of the changes that may happen to the legal resources and affect the case description templates in the Knowledge Warehouse. The design of the database for Knowledge Warehouse supports the solution that in the case of statutory changes affecting only parameters (e.g. number values for levies, taxes, date of deadlines, institution names etc.) changes are made automatically in case description templates under human supervision. The ILS as provider of the content of legal resources will automatically send a notification to the organization that is responsible for the content of those case description template that are affected by changes to ensure that the necessary changes will be made in the related case description template. In the case of totally, new legal resource that cannot be linked to any previously codified legal resources, a responsible public officer of the Prime Minister office will be contacted; the responsible public officer will initiate the necessary amendments of the database. The connection between *UCEDMS* and Knowledge Warehouse warrants that users of the Knowledge Warehouse can directly use the forms and documents stored in *UCEDMS* if the related case description has supported by business processes of public administration within *UCEDMS* . In the case of a correct user authentication, the citizen can initiate the case by completing the related form. The Knowledge Warehouse provides both citizens and public officers with information on case descriptions relying on the related legal resources. However, the various legal resources on public administration, on regulation of processes and procedures, and citizens' problem solving cannot be mapped onto each other mutually. For this reason, in order to assist the public officers and the citizens, the Knowledge Warehouse employs a higher-level abstraction of concepts within public administration and life events of citizens; this approach yield the opportunity that relevant solutions of the problem can be found without knowing the exact technical and legal terms linked to the particular situation. The basis of the operation of semantic search services that handle complex and abstract concepts is the creation of a network of relationships among the case descriptions in a graph database, the building-up of a thesaurus, taxonomy, and ontology. The information, documents and other content stored in the Knowledge Warehouse will be organized in a unified framework, namely, the interrelated cases, the legal resources and their structure, the client's life events and there is an opportunity to assign the adequate business process of public administration (where such a supporting option is available) in concert with external, related information systems (*ILS*, *UCEDMS*). Beside the continuous improvement of the Knowledge Warehouse that is supported by the before-mentioned tools, there is feedback option that is available to the public officers for each case description. The thesaurus, taxonomy, the legal and domain ontology that describes the links among individual concepts and the relationships of other knowledge elements that are related to concepts (as axioms, rules), moreover the semantic search together make sure that responses from Knowledge Warehouse are as accurate as possible for both citizens and public officers. Searching for individual words and phrases based on traditional search procedures can result in too many hits due to the number of case descriptions and related legal resources that make it much more difficult to find significant information, make the job of public officers more complicated. Ontology and semantic search significantly improve search efficiency, thus reducing time-consuming activities. The search service of Knowledge Warehouse takes into account the ongoing change in citizens / client's requirements. The on-line interface will provide the semantic search service that helps citizens find the relevant case description, document template, or related legal resources they are looking for. The Knowledge Warehouse enables legally registered and authorized organizations to provide their employees with an online editorial interface which supports the filling out the placeholders of case description templates, furthermore linking together of relevant legal resources, document templates, and case descriptions. The user interface for editing assists the process of definition of case descriptions, storing it in the Knowledge Warehouse, verifying and validating of case description by the responsible organization's staff, and approving by the public officer within the Prime Minister's

Office who is responsible for the Knowledge Warehouse. Organizations who are responsible for case descriptions will be notified about changes in related legal resources, about changes that were automatically carried out, and feedbacks from public officers within Citizens' Relationship Management through the editorial interface.

The Knowledge Warehouse requires a scheme for organizing the work of public administration to sustain the actuality of legal resources in force by members of responsible branches and sectors of the Government.

This scheme for organizing the work related to Knowledge Warehouse demands organizing of business processes of public administration such a way that tracks changes legal resources and deals with the textual information related to the given procedural act. These business processes of public administration transform the changes appearing in legal resources published in the ILS into the form that can be fed into the information system that contains the current information and knowledge by the time the legal resource enters in force.

2.2. Legal Resources Represented by XML

The *Integrated Legislative System* (*ILS*) and *National Legislation Register* (*NLR*) will apply the standards of MetaLex [11] that has been accepted by CEN/ISSS (European Committee for Standardization). Under the concept of legal resource is understood the legislation (a set of laws passed by a parliament), and all written documents that are created by a legislator and that elucidate and justify the legislation; furthermore legal rules as regulations, resolutions, directives, circulars, internal instructions created by various levels of authorities. MetaLex XML schema is intended to offer a lowest common denominator among the disparate jurisdiction-dependent and developer-specific representation of legal resources and to enforce uniform view on legal resources existing in the form of legal documents and support the interoperability and data exchange among the diverse sources to assist information system development. Fulfilling the before-mentioned set of prerequisites, MetaLex allows for XML schema extension, enhancing meta-data, cross-referencing among elements of XML documents, building up composite XML documents utilizing the referencing options, a change management mechanism that conforms to version handling that valid within legal environment, moreover a naming convention (elements, attributes of XML representing meaningful parts of legal documents) for development of software that realizes the goals.

The names of legal resources and legislative bibliographic entities should be linked to an identifying *internationalized resource identifier* (*IRI*) whereby (1) the document can be identified, (2) another document can be cited, (3) components of the document can be included.

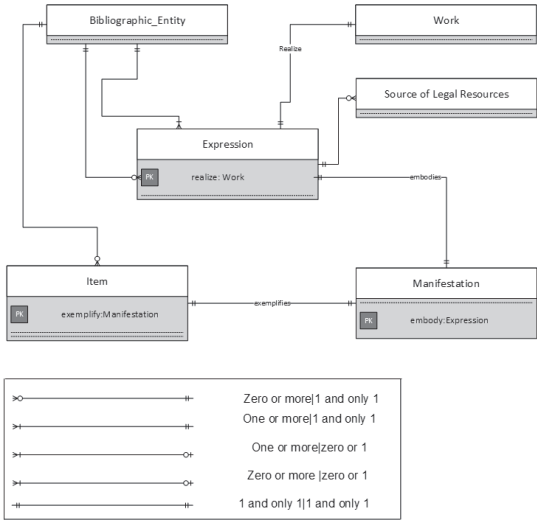

Figure 2: Relationships of Major Concepts within MetaLex (source [11])

MetaLex rigorously differentiate the source of legal resources and laws as released work from the expressions over time, expression from its distinctive manifestations of the specific legal resources; furthermore from items that are the physical representation instances of a manifestation.

There is a localized version of MetaLex XML schema customized to the jurisdiction by *Integrated Legislative System* (*ILS*) and *National Legislation Register* (*NLR*). The customized XML schema exploits the options for enhancement of meta-data, defining an adequate content model, and elaborating a scheme for referencing and cross-referencing. *Integrated Legislative System* (*ILS*) and *National Legislation Register* (*NLR*) comply with the standard of ELI (European Legislation Identifier) that is in fact the well-known web reference schema (IRI/URI/URL/URN), there are subtleties that should consider however the resolutions of the related problem areas typically belong to the technical and implementation level.

As it can be seen in the figure (Figure 2) the taxonomy of notion commences at concept of "*work*" as rule codifications (law, regulation directive, resolution et.), i.e. the work of legislation. The actual textual content of a legal resource comprises the next level of abstraction, the "*expression*" then the manifestation, "physical representation" of the text that incorporates the codified work of legislation in the form of printed paper, PDF, HTML. Within the manifestation there are options to refer to parts, articles, sections, paragraphs etc. As it can be seen, in spite of the conceptual approach in the case of legal resources the approach concentrates on primarily on syntactical components. Nevertheless, there is an ontology that was defined so that the formal aspects of legal resources are placed into conceptual framework that provides the opportunity to build up an ontology that deals with semantical aspects of legal resources, case descriptions and the related life-events of citizens.

2.3. Relationship Between the Knowledge Warehouse and the Integrated Legislative System (ILS)

Beside the legal knowledge that appears in the form of laws and other resolutions, regulations – i.e. legal resources –, there is procedural knowledge within public administration that is similar to case-law in certain sense, thereby a semantic layer is required within the hierarchy of ontologies that can represent and grasp the legal knowledge following Tim Berners-Lee's stack of semantic tiers [3]. The technical terms that are used within case description for handling life-events of citizens and the search terms that are employed by citizens as laymen differ profoundly. Therefore, two parallel ontologies are required that support the semantic search and information retrieval. Firstly, the citizen depicts of the life-event he or she is personally involved. An ontology including the concepts of citizens is used to arrange the input data then the system with the help of ontology directs the citizen to submit the relevant characteristic of the case at hand. An ontology on legal concepts, business processes of public administration, and on the administrative procedures is required that structures case description templates, forms and document templates into the taxonomy of notion and makes possible to maintain the conceptual and logical relationships among them. The ontology for citizens' terminology and the ontology for legal notion are strongly coupled to each other.

In order to execute complex queries of citizens and public officers on case description templates it is required to bind the generic and domain level ontology concepts to factual level, domain-specific ontology that ensures the accessibility the instances within the extension of concept classes.

Integrated Legislative System (*ILS*) stores and publish the actual legal resources, the legal resources in force, and the changes to legal resources, moreover the new legal resources. From the viewpoint of the Knowledge Warehouse the legal resources that deals with relevant issues of public administration should be considered to update the references and check the consistency of ontological models, and if necessary initiate the required modifications at all levels of ontology automatically or semi-automatically. As the MetaLex based structure for meta-data is grounded in the conceptual classes for describing legal resources, it is rather a conceptual, ontological description of the syntactical relationships of components within legal resources. However, the case management related to life events of citizens requires a semantic interpretation of both case description templates and legal resources referenced by them. The semantic aspects can be attached to the overall structure through a disciplined hierarchy of ontologies where through the lowest level the documents of case description templates and existing cases can be accessed within the document database.

The components of a three level ontology can be as follows:

- Generic legal ontology;
- Domain ontology of public administration;
- Domain-specific ontology for life events and case descriptions

The refinement of ontologies means that the top level classes of legal ontology conform with the MetaLex naming and structural conventions of components and contents. The domain ontology and the domain-specific ontology allows the definition of semantic content whereby the documents of case description can be queried semantically, i.e. the deduction and subsumption that are represented within ontologies can be used by the reasoner subsystem.

3. Conclusion

The above outlined approach makes possible that the activities of citizens and public officers in a Citizens' Relationship environment can be supported at higher quality level by exploiting the semantic representation of concepts in relevant legal resources and case descriptions. The semantic mapping require serious cognitive and development efforts but it is possible for process improvement within public administration.

4. Acknowledgement

This paper has been written with the support of the National University of Public Service in the framework of the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development for Establishing Good Governance" - Ludovika Digital Governance Research Group.

5. References

[1] APOSTOLOU, D., STOJANOVIC, L., LOBO, T., & THOENSSEN, B.: Towards a semantically-driven software engineering environment for egovernment. E-Government: Towards Electronic Democracy, 157-168. (2005)

[2] BARABUCCI, G., CERVONE, L., PALMIRANI, M., PERONI, S., & VITALI, F.: Multi-layer markup and ontological structures in Akoma Ntoso. In *AI Approaches to the Complexity of Legal Systems. Complex Systems, the Semantic Web, Ontologies, Argumentation, and Dialogue* (pp. 133-149). Springer Berlin Heidelberg (2010).

[3] BERNERS-LEE, T.: The Semantic Web. Accessed: 2017-12-08, https://www.w3.org/2002 /Talks/04-sweb/slide27-0.html

[4] BOELLA, G., et al. Integrating Legal-URN and Eunomos: Towards a Comprehensive Compliance Management Solution. In: AI Approaches to the Complexity of Legal Systems: AICOL 2013 International Workshops, AICOL-IV@ IVR, Belo Horizonte, Brazil, July 21-27, 2013 and AICOL-V@ SINTELNET-JURIX, Bologna, Italy, December 11, 2013, Revised Selected Papers. Springer, 2014. p. 130.

[5] BOER, A., HOEKSTRA, R., DE MAAT, E., HUPKES, E., VITALI, F., PALMIRANI, M., RÁTAI, B.: CEN, Metalex Workshop Agreement (August 28, 2009) (proposal). Accessed: 2017-12-08,

[6] https://www.researchgate.net/publication/228804628_CEN_MetaLex_Workshop_Proposal .

[7] BOER, A., WINKELS, R., VITALI, F.: MetaLex XML and the Legal Knowledge Interchange Format. In: Casanovas, P., Sartor, G., Casellas, N., Rubino, R. (eds.) Computable Models of the Law. LNCS (LNAI), vol. 4884, pp. 21–41. Springer, Heidelberg (2008).

[8] BREUKER, J., BOER, A., HOEKSTRA, R., SARTOR, G., RUBINO, R., PALMIRANI, M., GORDON, T.F.,WYNER, A., BENCH-CAPON, T.: Deliverable 1.4 of the European Project ,

ESTRELLA – OWL Ontology of Basic Legal Concepts (LKIF-Core). Technical report, University of Amsterdam, Bologna, Liverpool and Fraunhofer FOKUS (2007).

[9] BREUKER, J., BOER, A., HOEKSTRA, R., VAN DEN BERG, K.: Developing content for LKIF: Ontologies and frameworks for legal reasoning. In van Engers, TM, ed.: Legal Knowledge and Information Systems. Jurix 2006: The Nineteenth Annual Conference. Volume 152 of Frontiers in Artificial Intelligence and Applications (2006).

[10] BREUKER, J., HOEKSTRA, R., BOER, A., VAN DEN BERG, K., RUBINO, R., SARTOR, G., PALMIRANI, M., WYNER, A., AND BENCH-CAPON, T.: OWL ontology of basic legal concepts (LKIF-Core). Deliverable 1.4, Estrella, (2007).

[11] CEN: MetaLex, Open XML Interchange Format for Legal and Legislative Resources, Accessed: 2017-12-10 http://metalex.eu/

[12] MOLNÁR B, BENCZÚR A.: A Document Centric Approach for Analysis and Design of E-government Systems. In International Conference on Electronic Government and the Information Systems Perspective 2015 Sep 1 (pp. 319-333). Springer, Cham.

[13] OASIS.: LegalXML Lawful Intercept TC, Accessed: 2017-12-08, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=legalxml-intercept

[14] PERISTERAS, V., TARABANIS, K.: The governance enterprise architecture (GEA) high-level object model. *Knowledge Management in Electronic Government*, 2004, 101-110.

[15] Supreme Court of Western Australia, in partnership with the Department of Justice. Proposed XML Schema Definition of Supreme Court Judgements (June 15, 2011), Accessed: 2017-12-08, http://www.legalxml.org/workgroups/jurisdictional/australia/uncopies/UN_10013_2000_06_27.htm

[16] VITALI, F.: Akoma Ntoso Release Notes (1997), Accessed: 2017-12-08, http://www.akomantoso.org

WHICH BARRIERS HINDER A SUCCESSFUL DIGITAL TRANSFORMATION IN SMALL AND MEDIUM-SIZED MUNICIPALITIES IN A FEDERAL SYSTEM?

Markus Jakob[1] and Helmut Krcmar[2]

DOI: 10.24989/ocg.v331.12

Abstract
Digitalization nowadays is a frequently used buzzword in private industries as well as in the public sector. Digital services are not rocket science anymore. The technology is ready and concepts for using them in public administration exist. Recently, e-government laws were enacted all over Germany to foster and structure the digitalization of administration. Basically every authority is affected by the regulations. So are the small and medium-sized municipalities. Their structure is heterogeneous: Many of them have a small administrative organization and suffer e.g. from small budgets and a lack of experts. To develop an understanding of what the specific challenges regarding digitalization in small and medium-sized municipalities in a federal system are, we conducted a series of 12 expert interviews across municipalities of different sizes in one German territorial state. The analysis of the answers provides an idea of the municipalities' strategical and technical possibilities and their opinions on what would be beneficial for their further development in general and specifically with regard to the implementation of e-government laws. The acquired findings enable future research regarding a need for action and beyond to identify recommendations for action as well as to support municipalities in handling future digital challenges.

1. Introduction

Technical progress offers more and more possibilities for business and daily life. Consumers as well as companies have already gotten used to the skills and flexibility new technologies provide. Ordering goods online or communicating via diverse channels, where e-mail is one of the old-fashioned variances, are only basic examples. However, new technical opportunities are fostering higher expectations: Expectations regarding the daily life of working, shopping and enjoying one's spare time. Most of the time little technical helpers support one's daily doings. We can order tickets via smartphone and track our running distance, call friends and share pictures of a hiking trip with the world. If there is a problem, the fastest way to get a reaction from a provider of a faulty service is to complain via the social media channels of big companies. Normally there is a response in less than one day. Therefore, it is not surprising that expectations regarding the communication with and services of public authorities are also on the rise [9]. Subsequently, consumers and companies have specific expectations regarding the way they communicate not only with their friends or business partners, but also with public administration. Especially in Germany, there is substantial dissatisfaction with the progress and speed of digitalization within public administration [9] [18]. One way of communicating with public administration is by using the online services public administration offers. However, as the German political system is a federalism [3] and therefore the

[1] fortiss GmbH, Guerickestraße 25, 80805 München, Germany, jakob@fortiss.org, www.fortiss.org
[2] Technische Universität München, Boltzmannstr. 3, 85748 Garching, Germany, krcmar@in.tum.de, www.winfobase.de

power is divided into different layers, public administration as one "single person of contact" does not exist in Germany. For example, the federal system alone has three layers with different areas of responsibility ("Bund," "Länder," "Kommunen"). Additionally, each layer has many departments or authorities (e.g. "Ministerien" or "Landesämter"). The layer in which consumers and businesses have the most points of contact is the municipality level ("Kommune"), where in Germany approximately 70 administrative procedures [14] exist. People need to contact the municipality when they need an identity document or when they move from or to a city. Therefore, municipalities are often at the forefront when something is not working as expected by the client, for example, when a citizen wishes to get in touch to make quick use of municipality services online.

Starting from this practical problem of dissatisfaction, a potential solution is a more digitalized administration that can offer flexible services to its customers - citizens as well as companies. German politicians have been conscious of the relevance of digitalization and therefore push digitalization in every sector. Also the digitalization of administration is fostered [15]. There were legal barriers like regulations or laws that hinder it or, make it at least harder to digitalize [2]. To face these issues, almost all state governments in Germany as well as the Federal Republic of Germany, recently came up with e-government laws (e.g. EGovG) to regulate and drive IT innovation within public administration and to communicate with citizens and companies [1]. The State of Bavaria also implemented such legislation, the Bavarian e-government law (BayEGovG). With some exceptions, the law applies to every kind of public administration, thus to ministries as well as to state offices and municipalities (Art. 1 BayEGovG). Among other duties, the law requires implementation of IT security concepts or digital access to administrative services by the year 2020. In contrast to private communication or interactions with private companies, implementation in public administration encounters diverse and very specific requirements. Of course there are legal regulations, but also the federal system, departmental sovereignty ("Ressorthoheit") and local self-government ("kommunale Selbstverwaltung") [10] come with certain provisions [12] that may hinder quick digitalization. As the majority of public administration consists of small municipalities [7], we decided to choose this group as our peer group. E.g. in Bavaria 1,831 out of 2,056 municipalities have 10k or less inhabitants; throughout Germany it is a quite equal ratio: 9,516 out of 11,092 are smaller than 10k inhabitants.

To get an overview of the possibility of implementation of the new legal regulations as well as the possibility of future changes, we investigate the vitality of the IT infrastructure and organization in small and medium-sized municipalities. We want to elaborate whether small cities are able to meet the requirements, and if they meet them on time, how they plan to comply with the plan and whether they are open for cooperating with other municipalities. The following parts of this paper are structured as follows: First, the research methodology of gaining empirical data via expert interviews is briefly described (Chapter 2). Second, the results of the interviews are presented and split into ten different barriers based on the interviews (Chapter 3). Finally, the conclusion (Chapter 4) and limitations as well as possibilities for future research in this area (Chapter 5) are appended.

2. Methodology

2.1. Interview guidelines and interviewees

The study reported here was designed to obtain knowledge about the vitality of the IT departments of municipalities. Among other results, we expect to find the status quo of the law requirements

municipalities have to meet regarding the BayEGovG, information about the question of whether support is needed and how well municipalities are organized regarding further IT innovations.

In designing the guidelines we basically followed the guidelines of Diekmann [8] and Gläser & Laudel [11]. One principle we followed is to first have a clear definition of what our objectives are; based on this, we could start to design the interview guidelines. However, the type of questions depends on the answer you want to get and the people you want to ask. The question should be short but accurate, the wording should not be too complicated and double negative questions should be avoided.

Due to the fact that we want to know how to assist municipalities on their way to digitalization and whether the BayEGovG provides a framework that assists this plan, the interview guideline is aligned to the requirements of the law. Therefore, we ask about the fulfilling of certain legal milestones that the law sets [e.g. implementation of e-government services (Art. 4 Abs. 1 BayEGovG) or an IT security concept (Art. 10 Abs 2 BayEGovG)]. Additionally, we are interested in facts like a dedicated implementation strategy or a vague plan or whether they would need guidance for assistance and if so, what kind. Beyond that, we want to know about general indicators of the IT organization, like the number of full-time equivalent (FTE), the IT budget, drivers of innovation, the motivation of the people (employees and politics) and whether the costs of IT investments are barriers that prevent the implementation of a certain technique. Further, we are interested in finding out municipalities' attitudes regarding any kind of IT cooperation [13]. Scientists from the field of e-government as well as other fields in the information systems sector have reviewed the interview guideline.

2.2. Interview partners and analysis

In Bavaria, 2,056 municipalities with 232 inhabitants all the way up to 1.4 million run their services. The size of a municipality has significant impact on the number of people working in the IT department and thus on the level of know-how [16]. While using a classification for evaluating the questionnaire-based survey, we expect a more homogenous result over all questioned municipalities. Some literature exists for the classification of municipalities for different reasons, like classifying according to economic or social parameters [4]. In our case, the structure of the citizens is less important than the structure of the administration itself. Hence, we decided to classify the communities according to their size in terms of the number of inhabitants and believe that this is representative of the size of the administration. Following [19] and official statistics, we classified the Bavarian municipalities as follows: 1 to 2,000, 2,001 to 5,000, 5,001 to 20,000 and more than 20,000 inhabitants. We choose not to make a class for bigger cities, as the majority of municipalities (>96 %) has 20,000 or less inhabitants.

To get a representative number of interview partners, we choose to take 1% of all Bavarian municipalities, which is around 22. Additionally, we took one district ("Landkreis") and one county ("Regierungsbezirk") into consideration to cover all types of communes. The 22 municipalities were broken down by the regular distribution of all 2,056 within the Bavarian counties. At first, every chosen commune was contacted in order to get an appointment for a telephone interview. Therefore, an e-mail with general information about the scientific work, the interviewer and the topic was sent to the managing director of the chosen communes. Unfortunately, the response rate was poor, with only one out of 22 municipalities responding and offering an interview immediately. All other communes were called by the interviewer. Most of the called persons were open for discussion, but not all of them were willing to give an interview. Finally ten out of 22 completely

rejected the request for an interview. The given reasons for not taking part in the interview series were (a) not having enough time because of the workload or (b) no interest due to many recent interview and survey requests. Before the actual interview started, the scientist asked whether the conversation could be recorded for scientific reasons. All participants agreed and the interview started with the first question block, the general questions about the IT organization. In addition to the recorded interview, the scientist also took notes to have a first analysis, as well as to document which parts of the interview guideline have already been ticked off.

The recorded interviews were transcribed word-for-word and the interview texts were analyzed with the help of qualitative content analyses [17]. The categories for this article in which we want to investigate the barriers that hinder a successful digital transformation were close to the e-government's laws' targets. Indeed, if there was a target not fulfilled by a municipality, they usually named a reason and described it very well. These named reasons were our hints for the barriers they had. Subsequently, we continuously collected these causes and classified them regarding their topic (e.g. politics, strategy, resources). Afterwards, similar ones were clustered and framed in such a way that the original meaning was not lost, and we described each of them.

3. Results

In the results section, we provide barriers that hinder small and medium-sized municipalities in developing an up-to-date status of digitalization. The following results do not mean that the mentioned barriers were named in each interview or that all or most of them always appear. If one of these barriers appears within a municipality, the chance that it hinders a successful digitalization is relatively high. For example, not every municipality we talked to has a missing awareness at the local politics level. But when politicians do not care about developing a digitalization strategy, it will not be pushed and will not happen. In summary, we found ten barriers that are categorized into two categories depending on whether their origin is internal or external. Hereby, internal means caused by the municipality itself and external means caused by some external organization, institution or political layer. Because of the high frequency of internally caused barriers, we made three subcategories. These subcategories describe the reasons of the internal origin: Strategic, politics and resources. Strategic in this context means that a barrier has to do with the strategy for future decisions and the task of the authority [5]. Politics relies on political decisions and resources means that there are not enough or not the right resources available. It can also be connected to the employees, the knowledge they have, the decisions they make or the attitude they have.

Barriers	Origin			
	External	Internal		
		Strategic	Politics	Resources
Frustration leads to a "Wait-and-see approach"	X			
Missing IT strategy		X		
No plan for implementation of the BayEGovG		X		
Little knowledge about the BayEGovG, its duties and deadlines				X
No priority at local politics level			X	
Uncertainty about how the challenge should be faced		X		
No strategic cooperation		X		
No budget for IT projects			X	
No relevance seen for citizens in smaller municipalities				X
Lack of IT experts				X

Table 1: Results: Barriers and their origin

3.1. External

One reason for a slow digitalizing of communes we found during our interviews is frustration – frustration that comes from unsuccessful past projects that were not completed in a satisfactory way, although the administration spent a lot of effort and resources. Some of the interviewed communities have already made bad experiences with the implementation of recommended IT services like DE-Mail. In this case, they invested resources to figure out how to implement and use the DE-Mail for their own administration. However, the technique is not in use. Communities are disappointed because of the lost resources. Therefore, they have decided to wait and see regarding future IT service projects. It became clear in the interviews that as soon as better or best practices exist, they will also invest in a new feature, which could be a service or technique. In summary, failed projects without responsibility for the failure lead to frustration and hinder a successful digitalization.

3.2. Internal

3.2.1. Missing IT strategy

During the interviews, we asked the municipalities whether a strategy for IT exists in the broadest sense. We intended to get an idea about the strategic relevance of IT. Additionally, we wanted to know whether there is one and whether it is associated with political targets. Eight out of twelve interviewees stated that there is no strategy or that the strategy is not linked to politics. Existing strategies, in the broadest sense, can have different reasons. In bigger cities with a dedicated IT department, an IT strategy is common. Smaller ones also have created such a strategy, which includes an exchange of hardware and software, as well as implementation plans for certain applications. Another variance is that an auditing association determines some issues, and the fixing of these could be used as a medium-term strategy. As the auditing association [6] does not visit every municipality regularly and offers only a small variation of tasks regarding information

technology, this kind of strategy needs a bit of fortune to get planned. When there is no strategy or at least a low-level idea of what to do, the IT cannot act as an enabler [5]. Therefore, the complete absence of an IT strategy also hinders successful digital transformation.

3.2.2. No plan for implementation of the BayEGovG

A strong connection to the IT strategy overall has the dedicated implementation of the requirements of the BayEGovG, as they impact most of the IT concerns of a municipality. We have chosen the BayEGovG as a guideline for the interviews, as this law has certain duties and deadlines and thus all municipalities should face the implementation. Unfortunately, most of the interviewed communes do not have a plan for implementation. They partly know the requirements of BayEGovG, but have neither a plan with regard to the necessary steps nor with regard to the legal deadlines. Only one municipality in our evaluation stated that they have an implementation plan. Also, the option of a realization plan for the next step was among the answers. In this case, the next step is the implementation of an IT Security concept. More precisely, this task has the highest attention in our peer group so far.

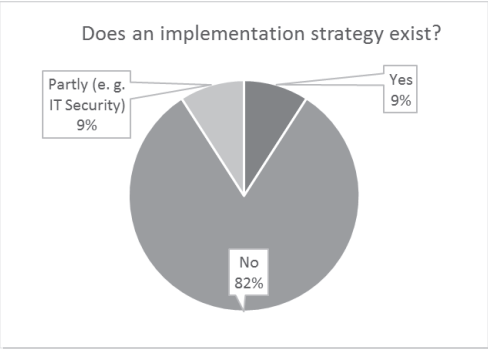

Figure 1: Existing IT strategy

3.2.3. Little knowledge about the BayEGovG, its duties and deadlines

The very low number of plans to realize the requirements of the BayEGovG is not surprising if we look at the next barrier we found. In the replies to the question regarding the knowledge of the BayEGovG and whether its duties and deadlines are known, we experienced some hesitant responses. Most respondents, but not all, have already heard about the law and only a few really knew about the content. Nevertheless, they had good explanations like less time or low priority. For example, one stated that every week an increasing number of law changes arrive on his desk. As IT does not have the same status as construction in a municipality, IT laws have a rather low priority. In summary, one could say that if the people do not really know about the law or about the deadlines, it will be hard to meet them or even make progress or define an implementation plan (3.2.2.) or an IT strategy (3.2.1.).

3.2.4. No priority at local politics

At the state or federal layer, experts for information technology or digitalization are often employed to bring their ideas to the politicians. Also, in big cities politicians have a professional structure for open questions in different disciplines. The smaller the entity, the fewer personnel and thus IT experts. Thus, in small municipalities, the local politicians are often left on their own. If they have neither the knowledge nor the experience in terms of digitalization, these topics often have less or no priority. Additionally, they have top priority topics like construction of buildings, such as schools, or infrastructure, such as streets or water distribution. Consequently, low-priority topics won't appear on their agenda. Some of our interviewed communes of course have drivers at the political level, but local politicians not prioritizing digitalization projects is definitely a barrier that hinders a successful digital transformation at the municipality level.

3.2.5. Uncertainty about how the challenge should be faced

Most of the asked persons stated that they do not have an implementation plan because they don't know how they should really start. Not only the start, but also the continuous fulfilling of the requirements of, in this case, the BayEGovG is a huge challenge for them. Most of them also have stated that they have no IT strategy nor do they have an implementation plan. One reason for that is that they do not know how to start or how to act at all. And because of the low priority at the politician level and fewer resources, there is not a plan of action and no action is taken at all. This does not mean that municipalities, in general, do not know how to act. Thus, uncertainty about how the challenge should be faced does not necessarily have to be a barrier, but can be a barrier.

3.2.6. No strategic cooperation

In case there are no internal resources, one solution to gain targets is a kind of cooperation. Cooperation exists in many variations. A cooperation, seen as working together to obtain a better, cheaper, faster result, could be a service provider for certain tasks or a higher instance or federal layer that takes over certain responsibilities. And, of course, a service provider as a shared service center that only takes over tasks for the member authorities is a possibility, too. The interviewed persons stated that in their authorities, some examples exist. Most of the time, it is the punctual partnership with a IT service provider only for specified tasks. These kinds of cooperations are no real strategic cooperation in which new ideas or future processes or applications are developed. Solely one municipality has a cooperation with their district ("Landkreis"), where the district takes over some strategic work, like "how should we implement the requirements of the BayEGovG?".

3.2.7. No budget for IT projects

Of course, most of the IT projects have a strong relation to money. That means a server or software and external services need to be paid for and employees earn money. In contrast to other expenses like the construction of a street or the building of a school, the financing of IT expenses is not that obvious. These days, online services most of the time are only additional services in addition to the originally paper-based service. They therefore result in additional costs. The money that can be spent is normally defined in the municipalities' budget in advance. Every additional project that is not budgeted in advance is hard to realize. Only four of our interviewed municipalities stated that they have a dedicated IT budget. All others include the expenses in the authority's budget, if necessary. In our investigation, a missing budget for IT projects is a barrier because there is no steady investment and development in this area. But this is necessary and indispensable if a municipality wants to implement the requirements of the e-government law.

3.2.8. No relevance seen for citizens in smaller municipalities

Another barrier we have heard of in our interviews has to do with the general perspective of public officials. From their point of view, there is often no relevance for online services for citizens, especially in smaller municipalities. As a reason, it was given that in smaller municipalities, compared to big cities like Munich, there are usually no queues in the town hall when citizens have to visit the public office. Another named reason for the irrelevance of online services was the extension of the municipalities' opening hours, which is a special offer for employed citizens, which enables them to visit the authority after work and handle their business with the authority in person.

3.2.9. Lack of IT experts

Smaller municipalities often do not have more than one person responsible for information technology, nor do they have a dedicated IT department. Based on this reason, along with "How many full-time equivalents (FTEs) work in your IT department?", we also asked "What percentage of FTEs are working in the IT department or are involved within IT topics?" At the municipalities we interviewed, on average there are 1.76 FTEs in IT personnel available. As the number of affected citizens is 20,216 on average and could be misleading, we reduced the IT FTE number to the common denominator of 10,000 citizens. Thus, in our investigation the number of FTEs responsible for IT topics is 0.85 IT FTEs per 10,000 inhabitants. This number even decreases to 0.33 FTEs if we only take the municipalities smaller than 10,000 inhabitants into consideration. In summary, they all found solutions to implement applications and run servers in cooperation or collaboration with service providers. But with a focus on the municipalities, IT employees have more tasks to fulfill, and so a lack of IT experts hinders successful digital transformation.

4. Conclusions

To sum up the identified barriers, one can point out some recommendations that would foster the implementation of the requirements of the BayEGovG in the short-term and, in the long-term, help small and medium-sized municipalities gain more competences and a higher degree of digitalization. The IT divisions no matter how big should have a better reputation and be integrated as an important member of the public authorities' strategic board. This comes along with more competences regarding future decisions that should foster IT strategy development, and to which the definition of a budget for IT or digitalization belongs. To implement this and, as a result, overcome most of the barriers, the acceptance of local politicians is an indispensable requirement. Nevertheless, all communities work with IT and most of them have digital (online) services for their customers: the citizens. However, where do they gain the expertise for such projects? They use different possibilities. The most common way is to make use of the help of an IT service provider. The service providers, generally speaking, want to sell their product. Products like, for example, a special application for public administration, need to be installed and maintained and people have to receive training courses to use the new product. Consequently, the service providers have to deliver all of these services. Another possibility for smaller authorities to gain knowledge is to work together with other communes. The administrative unit above a municipality is a district. Often the district assists the municipalities with the hosting of their website or data backup. One district out of our peer group's municipalities offers a dedicated agreement in which the district provides special IT services to the municipalities. In this case, 32 of 38 municipalities are taking part in this agreement. At the end, we have to state that the tasks of the Bavarian municipalities will be fulfilled anyway and in a very accurate way. It is not always very fast and with some circumstances for the customers, but the general work of the administration will be fulfilled. Moreover, it already works with IT because all of the officials we talked to stated that IT supports every department and almost every task. But that is not our focus. The focus of our study is how the service delivery can be handled more conveniently for both the sides of officials and customers with the help of digital assistance. The customers should not have double the work when entering their data, and the officials should be able to focus on tasks that are becoming more and more important for public organizations: Transparency, future strategy and further technical and organizational development.

5. Limitations and future research

One limitation of this investigation, of course, is the relatively low number of interviews that were conducted. Another issue that has an impact on the representativeness of this article is the view on just one state in one country. These limitations lead to the fact that it cannot be said that the list of barriers is final. Though both limitations should be targeted by future research to get a better overview on the reasons as to why digitalization in smaller municipalities is relatively slow developing.

To get a better overview and measure the efficiency, a broad-based study with more municipalities of different states in Germany could be useful. Further on, obviously the main target should be to find a solution to overcome the barriers this study came up with. A possible solution may be from an organizational matter from a higher federal level, which depends on political decisions. Also, it would be beneficial to have a maturity model to measure the actual status of e-government or digitalization depending on the size of the municipality or the authority in general.

6. References

[1] ALBRECHT, F., DITSCHEID, H. B., HECKMANN, D., KAMMER, M., LEUXNER, A., ORTMEYER, A., RIENASS, U., ROOS, D., ULRICH, C., SCHLIESKY, U., SCHULZ, S. E., & ZAPP, A. (2013). Das E-Government-Gesetz des Bundes *ISPRAT Dossier*. Frankfurt am Main.

[2] BÄHR, C., & DENKHAUS, W. (2016). Das Bayerische E-Government-Gesetz: Ein neuer Rechtsrahmen für die digitale Verwaltung in Bayern. *Bayerische Verwaltungsblätter - Zeitschrift für öffentliches Recht und öffentliche Verwaltung, 1/2016*, 10.

[3] BENZ, A. (1999). Der deutsche Föderalismus. In T. Ellwein & E. Holtmann (Eds.), *50 Jahre Bundesrepublik Deutschland: Rahmenbedingungen — Entwicklungen — Perspektiven* (pp. 135-153). Wiesbaden: VS Verlag für Sozialwissenschaften.

[4] CABALLERO, A., ALVAREZ, M., ABREU, J. L., CABALLERO, E., DEMIRALP, M., MIKHAEL, W., CABALLERO, A., ABATZOGLOU, N., TABRIZI, M., & LEANDRE, R. (2008). *Methodology for classification of municipalities in the state of Hidalgo, Mexico*. Paper presented at the WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering.

[5] DECARLI, P., FURTNER, E.-M., PROMBERGER, K., & SCHLAGER-WEIDINGER, N. (2014). *Gesellschaftliche, betriebswirtschaftliche und technische Anforderungen an die IT-Strategie einer Stadtverwaltung*.

[6] Der Bayerische Kommunale Prüfungsverband. Retrieved 29.11.2017, 2017, from http://www.bkpv.de/

[7] Destatis. (2017). Gemeinden nach Bundesländern und Einwohnergrößenklassen am 31.12.2015. Retrieved 29.11.2017, from https://www.destatis.de/DE/ZahlenFakten/LaenderRegionen/Regionales/Gemeindeverzeichnis/Administrativ/Aktuell/08GemeindenEinwohnergroessen.html

[8] DIEKMANN, A. (2014). *Empirische Sozialforschung* (B. König Ed. Vol. 9): Rowohlt Taschenbuch Verlag.

[9] e-Government Monitor 2017 - Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich. (2017). Berlin.

[10] GABRIEL, O. W. (1999). Kommunale Selbstverwaltung in Deutschland. In T. Ellwein & E. Holtmann (Eds.), *50 Jahre Bundesrepublik Deutschland: Rahmenbedingungen — Entwicklungen — Perspektiven* (pp. 154-167). Wiesbaden: VS Verlag für Sozialwissenschaften.

[11] GLÄSER, J., & LAUDEL, G. (2010). *Experteninterviews und qualitative Inhaltsanalyse*: Springer-Verlag.

[12] GREGER, V., WOLF, P., & KRCMAR, H. (2013). *Performance Management of IT in Public Administrations: A Literature Review on Driving Forces, Barriers and Influencing Factors.* Paper presented at the International Conference on Electronic Government.

[13] HANKEN, C. (2006). Interkommunale Zusammenarbeit. In M. Wind & D. Kröger (Eds.), *Handbuch IT in der Verwaltung* (pp. 393 - 402): Springer, Heidelberg, Germany.

[14] HEUERMANN, R., JÜRGENS, C., ADELSKAMP, P., & KRINS, T. (2018). Digitalisierung auf kommunaler Ebene *Digitalisierung in Bund, Ländern und Gemeinden* (pp. 51-98): Springer.

[15] HEUERMANN, R., TOMENENDAL, M., & BRESSEM, C. (2017). Digitalisierung in Bund, Ländern und Gemeinden.

[16] JAKOB, M., WOLF, P., & KRCMAR, H. (2015, 18.-19. Juni 2015). *Decision Objects for IT Cooperation Decisions in the Public Sector.* Paper presented at the 15th European Conference on eGovernment, Portsmouth.

[17] MAYRING, P. (2010). Qualitative Inhaltsanalyse. *Handbuch qualitative Forschung in der Psychologie*, 601-613.

[18] NORMENKONTROLLRAT, N. (2017). Bürokratieabbau. Bessere Rechtsetzung. Digitalisierung. Jahresbericht 2017 (Berlin, Trans.).

[19] SIEWERT, B., & WENDLER, T. (2005). Bundesverband Öffentlicher Banken Deutschlands (2005): Die Klassifizierung von Kommunen–ein Ansatz zur Vergleichbarkeit deutscher Städte und Gemeinden. Statistisches Bundesamt. *Wirtschaft und Statistik*, 885-890.

THE PUZZLE OF ICT DRIVEN INNOVATION IN THE PUBLIC SECTOR: HUNGARY´S CASE

András Nemeslaki[1]

DOI: 10.24989/ocg.v331.13

Abstract
Public ICT (Information Communication Technologies) investments do not necessarily result in improvement of effectiveness or efficiency regarding public services. Hungary has been spending around 1,2 billion Euros using funds from the European Social Cohesion and Structural Funds during the period of 2007-2018 for modernizing its public administration. Taking the investments into other sectors as a comparison, this means that more than 25% of ICT development projects go to the public sector, which is in the magnitude of the financial, commercial and media sectors of Hungary. While the effects of digital transformation are unquestionable in these latter sectors, effectiveness of public ICT spending is problematic. When we look at the measurement scoreboards used in the EU and UN, we find Hungary not even improved its position, but in some areas has lost competiveness and fell behind. In this paper we show using some elements of earlier findings in digital innovation studies on public administration, that four key factors should be analysed in detail to find out reasons behind this phenomenon, Infrastructural questions, although need constant development and improvement, do not seem to be key explaining factors of lack of productivity improvement. Nor the techno-legislative institutions seem to be obstacles in Hungary´s case, but rather some alignment in policy objectives and consistency.

Keywords: *digital innovation, public sector ICT, service and process innovation, Hungary*

1. Introduction

European digital cohesion is a pivotal question in order to increase competition and social wellbeing. Digital transformation of the public sector, government services and administration is in the heart of the reforms of European countries, not only to have cheaper governments and reduce administrative burden, but to exploit new opportunities of technology innovation. Several programs on the EU level provide guidelines, action plans and funding mechanisms for member states to implement public policies for digitalization and ICT based transformation, like the Digital Agenda, H2020, and the E-government Action plan.

In the course of these programs Hungary has been spending around 1,2 billion Euros using funds from the European Social Cohesion and Structural Funds during the period of 2007-2018 for modernizing its public administration. Taking the investments into other sectors as a comparison, this means that more than 25% of ICT development projects go to the public sector. While in the effects of digital transformation are unquestionable in these latter sectors, effectiveness of public ICT spending is problematic. When we look at the measurement scoreboards used in the EU and UN, we find the Hungary not even improved its position, but in some areas has lost competiveness and fell behind in several rankings. We put this dilemma as the main question of our research.

[1] Technical University of Budapest, nemeslaki@finance.bme.com

In this paper we enlighten the problem with the use of empirical data and systematically point out the areas which need to be addressed for future explorations, and for finding solutions for more effective ICT adoption in PA. Our focus is the special situation of Hungary, but using digital innovation as a theoretical framework we show that this analysis also has implications both beyond Hungary and for theory as well.

2. Problem statement and research question

Adoption of information communication technologies is a pivotal problem in public administration. While the concept of using information communication technologies (ICT) for improving efficiency of governmental services is as old, as ICT themselves [1] and often considered thoroughly researched [2], [3], we would like to develop arguments that this problem is highly relevant not only from a pragmatic public policy point of view but, very importantly, from a theoretical point as well.

Our key assumption is that low level of e-service adoption in governments, that is success in using ICTs for supporting public services, stem from lack of digital service innovation – an approach which considers the richness of the socio-economical change generated by technology development and allowing to go beyond the concepts of effectiveness and efficiency of existing services [4].

ICT deployment in public sector is triggered by policy objectives. Among many variations these are often administrative burden reduction, provision of better services, or enhancing economic development and innovation in the business sector. Attainment of these objectives are measured by aggregate statistical data combined using secondary and primary sources – the latter getting more relevant given the unique nature of digital transformation, which is often difficult to describe with standard macro economical statistics.

Performance of countries are measured and compared by several complex surveys. In this paper we are using two very commonly referred and used instruments two highlight the key problem what governments are facing. The first is the United Nations E-government Development Index (EGDI), and the second is the European Commissions Digital Economy and Society Index (DESI). In Hungary˙s case both indicate serious dilemmas of ICT investment in the public sector.

EGDI assesses countries based three equally weighted indices; a) On-line services index, b) Telecommunication Infrastructure Index and c) Human Capital Index (HCI). Each contain further sub-indices which are than normalized to a scale of 0-1. Based on these, a country ranking is also created, which is biannually presented in a detailed report analysing regions, special areas of public service and the detailed components of the indices. Since it is not the objective of this essay to analyse the EGDI surveys in detail, we draw the attention only to one of these analyses from the latest report available at the time of writing this manuscript [5].

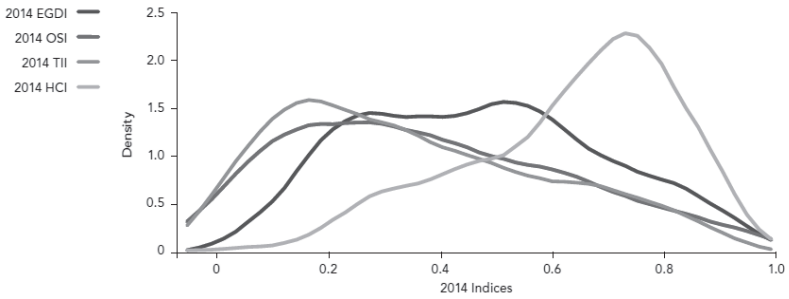

Figure 1: EGDI and its components [6]

As it is shown in figure 1 human capital scores are higher compared to the other two components. The lowest performing component is the Telecommunication Infrastructure Index (TII) which drags down the overall EGDI; while the Online Service Index (OSI) also trails in performance compared to the average value.

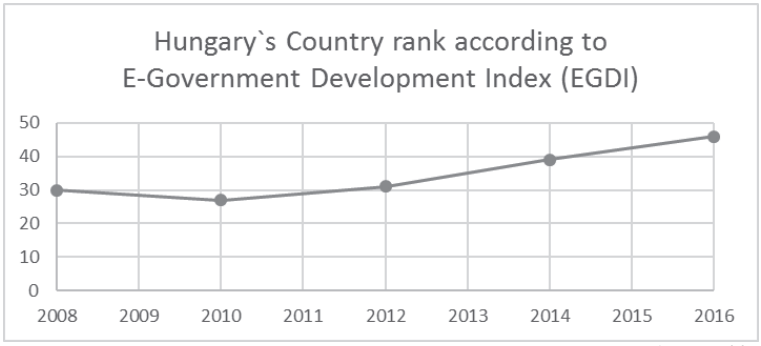

Figure 2: The assessment of Hungary´s public ICT effectiveness based on EGDI (*Created by the Author*).

When we look at Hungary´s assessment according to the UN EGDI reports – shown in figure 2– we see that the competitive position compared to others is steadily declining, from the 27th position in 2010 it fell back to the 46th in 2016. The performance is better, yet does not show relative improvement either, when we look at the other complex indicator, the DESI measure.

Hungary DESI	2014	2015	2016	2017
Connectivity and use	10,9	13,4	14,9	15,9
Digital skills	10,4	11,2	11,1	12,2
Use of Internet	6,3	7,15	7,67	7,76
Integration of Digital Technology	3,21	3,92	4,24	4,71
Digital Public Services	5,2	4,32	4,97	5,32
DESI RANK	**21**	**20**	**20**	**21**

Table 1: Hungary´s assessment according to the DESI indicators.

As we can see in table 1, DESI has five sub-indices: a) Network connectivity and use, b) digital skills, c) internet use, d) integration of digital technologies, and e) level of digitalized public services. Accordingly, DESI intends to assess a broad picture of ICT deployment than EGDI, it contains more data on enterprises and general ICT use amongst citizens. The last set of measures

focus on the narrow definition of e-government or public services collecting four set of data in this field, these are:

- number of individuals using public e-services,
- number of finished on-line transactions,
- use of open data
- use of on-line forms.

Amongst the 27 countries measured Hungary´s performance is steadily in 21-20th position, however when we look at this last measure – the digital public services – we found Hungary in the 27th place in 2017, which is a 7 places decline from the earlier measure in 2014.

In order to underline the real dilemma of the digitalization of public services we juxtapose the performance of EGDI and DESI measures with the financial investment which has been deployed during this period. As most Central Eastern European countries, Hungary also used mainly European Social Cohesion and Structural Funds for economic development. Two sources were dominant during the period of 2007-2013, and one source from 2013 onward.

- 173 million Euros were invested under the framework of the State Reform Operative Program in 2007-2013,
- 408 million Euros were invested as part of the Electronic Public Service Operative Program in 2007-2013 and
- 795 million Euros are partly spent and partly allocated during the period of 2014-2018 called Public Service Operative Program.

For comparison, we quote the IT services report of IDC (International Data Corporation) which indicated that the total market for development projects in IT services was 363, 403 and 442 million Euros in 2016, 2017 and 2018 in Hungary [7]. Taking the annual averages of the public IT development projects (114 million Euros between 2007-2018), this roughly indicates that annually 28% of IT project spending goes to the government sector. However, compared to other sectors (financial services, retail or the media industry) the results and effects are much less significant as our data has shown.

In order to investigate the "puzzle of IT adoption in the public sector", in the following sections we take a closer look at some data sources, in order to find explanations and at the same time indicate direction of further investigations.

3. Theoretical background of digital service innovation and the derived research model

There is a consensus in the literature that provision of public e-services is determined by the interaction of four areas. The two main ones, which seem to be taken granted in most cases are the IT infrastructure [8] and the techno-legislative institutions (regulations such as interoperability and

privacy) [9]. These two in our view are the "hard public administration requirements" or institutional determinisms. Beyond the hard requirements public organizations need "soft capabilities" as well. We consider two main sets of resources as part of these; first and foremost he human capacities of public administration to embrace the digital ecosystem at all levels – high level executives, mid-level management and personnel – including skills, knowledge and a mindset, [10], secondly the adoption of service oriented process management which efficiently cuts across silos of departments and organizations [11] [12]. Finally, awareness and adoption capability of citizens are essential to create a functioning public e-services ecosystem [13], [14], [15].

ICT infrastructure	**OK**
"Hard" infrastructure (network and equipment)	***OK***
"Soft" infrastructure (STEM graduates and ICT specialists)	***?OK?***
Techno-legal institutions (digital ecosystem)	**OK**
Laws and regulations	***OK***
Standards and procedures	***OK***
Service oriented process management and process reengineering	***?***
Client side awareness and re-engineering	***?***
Internal process redesign and process re-engineering	***?***
Organizational learning and leadership capabilites	**?**
Knowlegde based service innovation	***?***
Management and leadership for directing change	***?***

Table 2: Research Model for investigating the ICT innovation puzzle – Created by the Author

Based on these ideas we have established a research model presented in table 2. As far as data collection is concerned firstly, we looked at the latest report of the Hungarian Central Statistical Office which also serve as basis of for EuroStat data. We used the tables of "ICT equipment and use in public services", and throughout the paper we will refer to it as CSO-2016 [7] .

The second set has been a large scale representative survey conducted by the Hungarian Central Statistical Office the National University of Public Service (NUPS) during the last months of 2015 [16]. During the course of this 3800 citizens above the age of 18 were approached, of which 2160 successful data collection occurred at their homes. Cleansing and weighing for creating a representative set according to location, salary and gender has been calculated by the Measurement and Methodology Center of NUPS, and they generated tables for further analysis [17]. During the analysis we will refer to this as GGR-2016.

The third source, - and what we consider primary in our research - has been survey data of the Ministry of Interior which is responsible for e-service delivery. The survey was filled out by 1185 respondents, and the authors of the paper have processed the raw data by SPSS (Statistical Package for the Social Sciences).

4. Discussion of results

4.1. ICT infrastructure

Due to the continuous development of fix and mobile broadband technologies achieving a satisfactory network infrastructure is pivotal in the European Union. The Digital Agenda policy documents sets forth clear targets regardless both for coverage and penetration. Accordingly, by

2020 the availability to access 30Mbit/sec broadband at every household is articulated in the EU, while in 50% of these households the connection to 100Mbit/sec is targeted. In Hungary, the Digital Wellbeing Program brings the first objective even 2 years earlier – the 30Mbit/sec coverage is targeted for 2018. The same document is also ambitious in mobile networks; it articulates that Hungary intends to be in the front runners of the 5th generation implementors, although target dates are not announced.

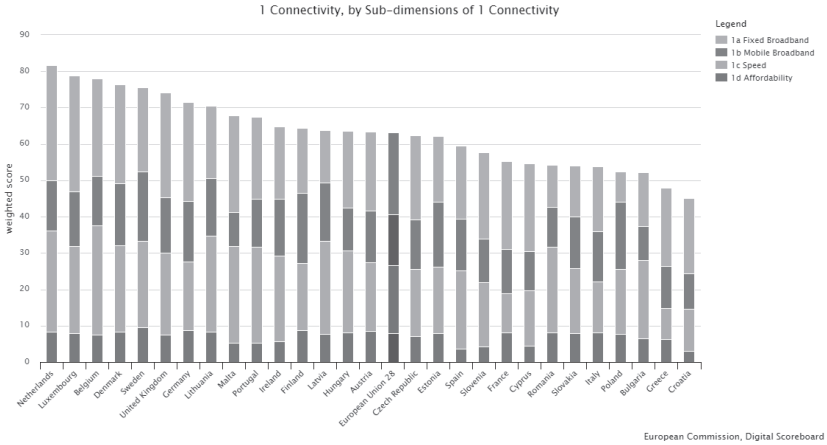

Figure 3: A glance look at ICT infrastructure – EU Digital Scoreboard 2017.

When we look at actual data describing connectivity, as is shown in figure 3, we can see that Hungary is basically average in EU comparison, actually improving its position between 2016 and 2017, closing up to its western neighbor, Austria.

In figure 4 we demonstrate that there are issues with STEM (Science-Technology-Engineering-Mathematics) graduates and ICT specialist. In Hungary´s case the STEM graduates are especially critical. compared to leading adopters such as Finland or UK, but even in regional comparison it looks suggestive that this area need further investigation. Basically all the new member states and the post-communist countries performing better in producing STEM graduates, and ICT specialists are also at the EU average.

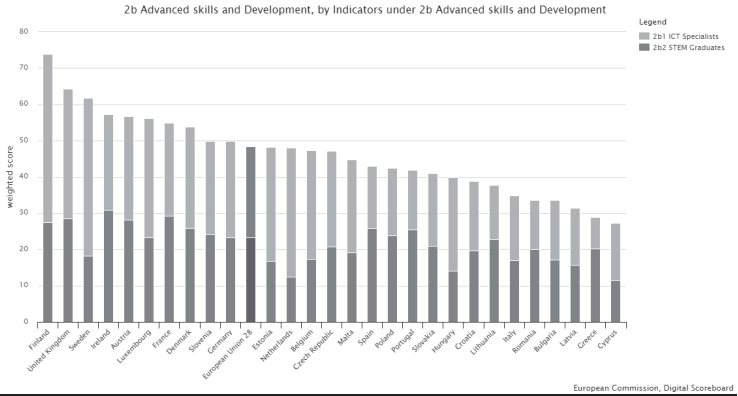

Figure 4: Special skills for ICT development: STEM graduates and ICT specialists – EU Digital Scoreboard 2017

The gap in STEM graduates are critical, because most of the new jobs generated by AI development and smart automation will require skills such as analytical, data processing algorithm design, etc. large taught in engineering, mathematics or other fields of sciences. However, I would argue that other fields will adopt these skills, and the STEM dilemma will be not that relavent in the future, since sociology, business, economics and other social sciences quickly adopt data science, applied digital skill development or other ICT related skills into their curriculum.

As a conclusion here, we might state that Hungary´s digital innovation dilemma is not rooted in infrastructure compared to other lead adopters, however the STEM-graduate dilemma might need to investigated in more detail.

4.2. Techno-legal institutions

Both qualitative expert opinions and empirical data underlines that the legislative institutional background is highly developed and enables digitalization a great deal in the Hungarian context. Hungary has put a lot of efforts for ensuring a modern and enabling legislative foundation for e-government adoption.

Key legislative milestones – the legal platform for interoperability

The Magyary Zoltán Public Administration Development Programme[2] contains the current situation of various public administration issues, actual problems to be solved, obstacles as well as strengths, potentials and real client needs. It initiates measures for interventions and several tools of development, such as one-stop-shops, redistribution of local and central powers, eGovernment, and human resource management. As a novelty, new building blocks had been introduced, the "regulated electronic administrative service" (Hungarian abbreviation: SZEÜSZ). SZEÜSZs are essential electronic services (front or even back office) from which complex electronic procedures and cases can be built. The governmental resolution contained the definition and basic requirements of the regulated electronic administration services, and also the list of the ones that the state (avoiding parallel developments) had to establish centrally. The mandatory SZEÜSZs are basically run by three major state organizations: the Central Office for Administrative and Electronic Public Services at the Ministry of Interior, the National Information and Communications Service Ltd. (NISZ Zrt.) and the Hungarian Post. Public administration institutions can use these services and integrate them into their own procedures. Some examples of regulated electronic administration services:

- Central Office for Administrative and Electronic Public Services: central authentication agent, timed client notification on electronic administration procedures, file validity register
- National Information and Communications Service Ltd.: government certificate authority (GOV CA), storage of e-documents, central form filling application
- Hungarian Post: secure delivery service, authentic conversion of paper documents into electronic form and vice versa

[2] http://magyaryprogram.kormany.hu

To ensure interoperability between all the services and to protect the interests of the clients, the governmental resolution calls for the setting up of the Electronic Administration Authority. Its main task is to permit and to harmonize the development and the cooperation of the regulated electronic administration services.

Focus and consistency of public policy

In figure 5 we depict the results of the COCOPS (Coordinating for Cohesion in the Public Sector) survey, which was investigating the question amongst 2013 policy experts on how important digitalization is in their respected areas. As we can see, amongst the 10 participating countries Hungarian policy experts indicated the lowest importance for digitization, although the variation between the most important average (Italy) and Hungary as the lowest is 1,5 points on the 7 Likert scale.

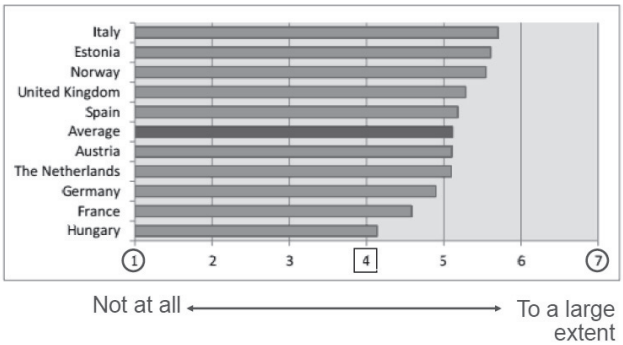

Figure 5: Importance of digital government according to the COCOPS survey [18].

4.3. Service oriented process management and process re-engineering

Client side awareness, use and skills

The key dilemma of Hungarian e-public service adoption is shown in figure 6. where we can notice that growth of on-line public service is basically determined by the use of internet users and their behavior; rate of access compared to the total number of population is not steeper or different in the two population, showing that there is no relative adoption gain from non-internet users for public e-service use in the period of 2006 and 2015.

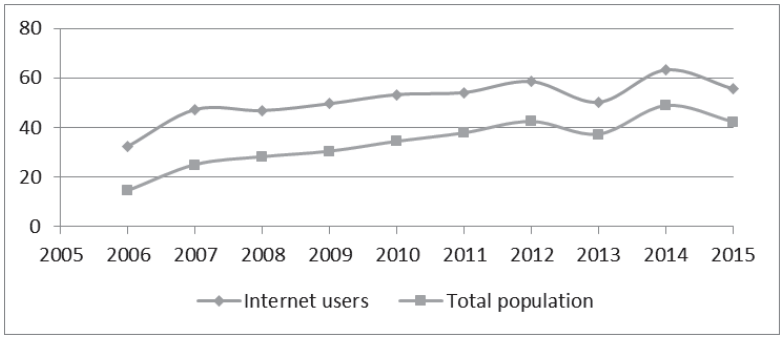

Figure 6: Usage of public e-portals % of internet users and % total population – Source: [7]

Although the number of e-portal users do not seem too much, according the DESI Hungary belongs to the EU average countries, and not very far from more developed as Austria and surprisingly much ahead of Germany. One key questions arises to what extent citizens aware of on-line services? In [16], a panel of 2000 users were asked on a scale of 1-4 (not aware – totally aware) about on-line services and results are shown in figure 7. The mean of the sample is 2,37 which is a "moderate level" of awareness.

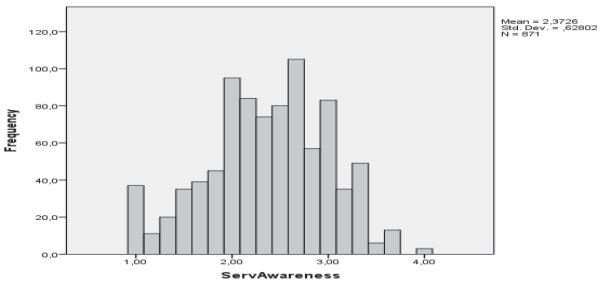

Figure 7: Awareness level of users about services - [16]

Channel preferences

As research shows in 2015, 71% of the Hungarian population got in touch with public services. Mostly once, (31,5%), twice (23,3%) and much rarely three times or more (only 16,2%). This indicates, that experience and judgement of public services is mostly based on few impressions – solutions need to be intuitive, simple to use, requiring little effort even at the first time [16].

Looking at channel use and satisfaction, in table 3, we can observe that preference of using personal channels is more than half of the respondents, but satisfaction is highest amongst the on-line channel users. This shows the importance of conversion; it seems like once on-line channels are explored they score better than the experiences with the personal or even with the phone channels.

Channels	Rate of usage (%)	Satisfaction (0-10)
Personal	58	8,04
Postal	21	8,34
Call center	4	7,19
On-line	18	8,62

Table 3: Channel usage and statisfaction – Source: [16]

Internal process design and re-engineering

However, the importance of the management instruments varies significantly across countries. This is especially the case for internal steering by contract. While this is rather widely used in Italy (4.94), the Netherlands (4.92) and Hungary (4.40), internal steering by contract is rarely used in Spain (2.69) and Estonia (2.90) [18].

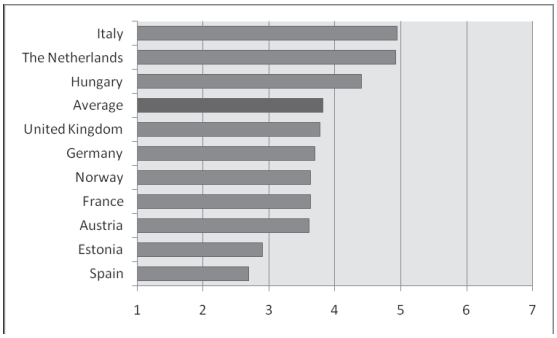

Figure 8: Importance of internal steering by contract (Q: To what extent is internal steering by contract used in your organization?; 1=Not at all, 7=To a large extent) [18]

Substantial country variation is also observable for the use of cost accounting systems. Such systems are rather widely used in the UK (5.25), Estonia (4.88) and Italy (4.54), but rarely used in Spain (2.86), Hungary (2.89) and France (3.15).

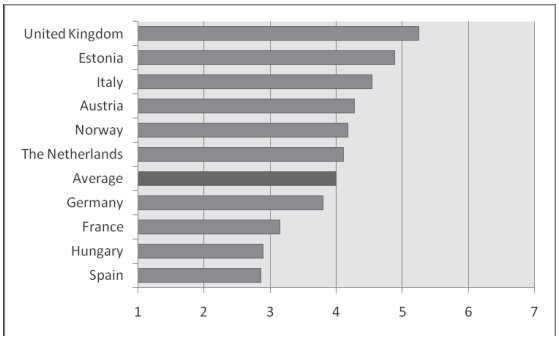

Figure 9: Importance of cost accounting systems (Q: To what extent are cost accounting systems used in your organization?; 1=Not at all, 7=To a large extent) [18]

4.4. Oganizational learning and leadership

The COCOPS survey participants from Hungary reported, that public administration reforms are demanding in terms of management, but they prove to be successful [18].

Four groups can be distinguished. In one group of countries, consisting of Germany and Norway, the senior executives assess the reforms in their country as rather successful (albeit to a moderate degree) and as not demanding enough, especially compared with their colleagues in other countries. In a second group of countries, consisting of the Netherlands, Estonia and Hungary, the senior executives also consider the reforms as rather successful, but at the same time as too demanding. In a third group of countries, the senior executives are less satisfied with the reforms in their policy field; they consider them as rather unsuccessful and too demanding. This is especially the case for France, where downsizing and mergers are important (and demanding) reform trends that challenge many dimensions of the French administration. Senior executives in Spain, Italy and Austria assess the reforms in their countries as less successful and as rather not demanding enough. When considering the demandingness of reforms, it is important to keep in mind that it is not necessarily the number of reform trends a country introduces that determines the perception of demandingness,

but that some reform trends (such as downsizing and mergers) are clearly more demanding than others (such as e-government or collaboration).

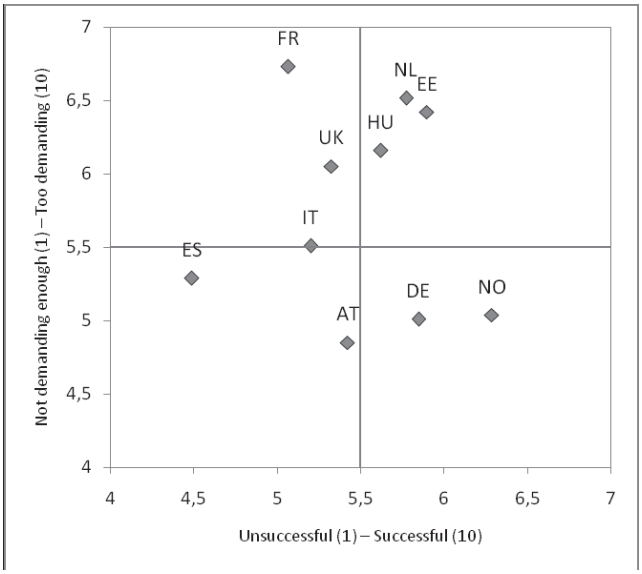

Figure 10: Dynamics of public sector reform: enough/too much vs. successful/unsuccessful [18]

Knowledge based service innovation

There are few data and research available on these dimensions of public organizations, especially in the context of technology driven or service driven innovation. Marton Gellén reported a study on interviewing and surveying Hungarian PA administrators on innovativeness and we summarize some of his results, which indicate the need for further study [19].

Cluster names	Innovative	No competition, no outsourcing	No innovation	Average	Competitive
Number of respondents in cluster	2,036	1,416	984	1,961	1,836
How important would you consider the following: hierarchy and sticking to chain of command?	4.49	**4**	3.08	3.93	**4.05**
(…) compliance to internal bylaws and internal instructions?	4.79	**4.52**	3.48	**4.53**	**4.55**
(…) relying on the expertise of the gov. civil service?	4.83	4.75	3.95	4.63	4.86
(…) impartiality, unbiased attitude?	**4.86**	**4.88**	4.16	**4.83**	4.91
(…) establishing competition among civil servants?	3.98	1.59	2.48	2.08	3.58
(…) precisely defining individual performance indicators?	4.69	3.89	3.21	4.19	4.49
(…) outsourcing of tasks?	4.17	1.42	2.64	3.75	1.83
(…) delegating tasks?	4.49	3.55	3.25	4.04	4.16
(…) involving gov. civil servants into decisions?	4.49	4.16	3.53	4.19	4.30
(…) involving colleagues as partners in work processes?	4.76	4.6	3.91	4.61	4.69
(…) cooperation with external professional institutions and with social partners?	4.58	4.01	3.33	4.35	4.43
(…) establishing occasional work connections with external institutions and with market players?	4.32	3.18	3.02	**3.87**	**3.92**

Figure 11: **Innovativeness of Hungarian public service organizations** [19]

5. Conclusions

We have shown using some elements of earlier findings in digital innovation studies on public administration, that four key factors of table 2. should be analysed in detail to find out in-depth reasons behind this phenomenon. Infrastructural questions, although need constant development and improvement, do not seem to be key factors, explaining the lack of productivity improvement. Nor the techno-legislative institutions seem to be obstacles in Hungary´s case, except some alignment in policy objectives and consistency.

Service oriented process management and knowledge driven organizational change, however, prove to be key obstacles for successful ICT adoption in digital governance.

6. References

[1] BANNISTER F ; CONNOLLY R, "Forward to the past: Lessons for the future of egovernment from the story so far," Information Polity, vol. 17, no. 3-4, pp. 211-226, 2012.

[2] JUKIC, T.; TODOROVSKI L.; NEMESLAKI, A. "Investigation of E-government Research Field: What Has Been Done and How to Proceed?," in *23rd NISPAcee Annual Conference*, Tbilisi, Georgia, 2015. May 21–23, 2015.

[3] ZABUKOVSEK, S; BOBEK, S; VOSNER, S; SEBJAN, U. "Bibliometric Analysis of E-government Research," in *Multi-Level (e) Governance: Is ICT a means to enhance transparency and democracy? CEE e-Dem and e-Gov Days 2016*, Vienna-Budapest, 2016.

[4] BARRETT, M.; DAVIDSON, E.; PRABHU, J.; VARGO, L. "Service Innovation In The Digital Age: Key Contributions And Future Directions," *MIS Quarterly,* vol. 39, no. 1, pp. 135-154, 2015.

[5] UNITED NATIONS, United Nations E-Government Survey 2016, New York: UN Department of Economic and Social Affairs, 2016.

[6] UNPAN, "United Nations E-Government Survey 2014: E-Government for the Future we Want," United Nations Department of Economic and Social Affairs, New-York, 2014.

[7] RANA, N.; WILLIAMS, M.; DWIVEDI, Y.; WILLIAMS, J. "Theories and Theoretical Models for Examining the Adoption of E-Government Services," *e-Service Journal,* vol. 8, no. 2, pp. 26-56, 2012.

[8] SZÁDECZKY, T. "Information Security - Strategy, codification and awareness," in *ICT Driven Public Service Innovation*, Budapest, Publisher of the National University of Public Service, 2014, pp. 99-112.

[9] KADAR, K.; "Good Governance: International Dimension", Budapest: National University of Public Service, 2015.

[10] DAVENPORT, T.: "Process Innovation: Reengineering work through information technology", Boston, MA: Harvard Business School Press, 1993.

[11] VANDER ELST, S.; DE RYNCK, F. "Diving in the Dynamics of Alignment Process in Public Organizations: Lessons for a Reconceptualized Alignment Framework," in *EGPA Conference*, Speyer, Germany, 2014.

[12] ALHARBI, A.; KANG, K.; HAWRYSZKIEWYCZ, I. "The Influence of Trust and subjective Norms on Citizens' Intentions to Engage in E-participation on E-government Websites," in *Australasian Conference on Information Systems*, Adalaide, 2015.

[13] LIN, F.; FOFANAH, S.; LIANG, D. "Assessing citizen adoption of e-Government initiatives in Gambia: A validation of the technology acceptance model in information systems success," *Government Information Quarterly,* vol. 28, no. 2, pp. 271-279, 2011.

[14] WELCH, E.; HINNANT, C.; MOON, J. "Linking Citizen Satisfaction with E-Government and Trust in Government," *Journal of Public Administration Research and Theory,* vol. 15, no. 3, p. 371–391, 2009.

[15] CSO, Az infokommunikációs technológiák és szolgáltatások helyzete Magyarországon 2015 (Status of ICT and related services in Hungary-2015) - in Hungarian, Budapest: Central Statistical Office, 2016.

[16] KAISER, T. Ed., "Jó Állam Jelentés (Good Governance Report) 2016 "- in Hungarian, Budapest: NKE Kiadó, Improved and Abridged Edition, 2016.

[17] CSUHAI, S. Ed., "Jelentés a Jó Állam Véleményfelmérésről (Report on the Opinion Survey of the Good Governance Report)" - in Hungarian, Budapest: NKE Kiadó, 2016.

[18] HAMMERSCHMID, G.; OPRISOR, A.; ŠTIMAC, V. "COCOPS Executive Survey on Public Sector Reform in Europe," Coordination for Cohesion in the Public Sector of the Future (COCOPS): www.cocops.eu, 7th Framework Programme, 2013.

[19] GELLÉN, M. "Bureaucrats As Innovators? Statistical Analysis On Innovative Capacity Within The Hungarian Central Civil Service," *Transylvanian Review of Administrative Sciences,* vol. Special Issue, pp. 38-54, 2016.

[20] MEDAGLIA, R. "eParticipation research: Moving characterization forward (2006–2011)," *Government Information Quarterly,* vol. 29, no. 3, p. 346–360, 2012.

[21] IRANI, Z.; WEERAKKODY, V.; KAMAL, M.; HINDI NITHAM, M.; ANOUZE, O.; EL-HADDADEH, R.; LEE, H.; OSMANI M.; AND AL-AYOUBI, B. "An analysis of methodologies utilised in e-government research: A user satisfaction perspective," *Journal of Enterprise Information Management,* vol. 25, no. 3, pp. 298-313, 2012.

[22] BROWN, D. “Electronic government and public administration,” *International Review of Administrative Sciences,* vol. 71, no. 2, p. 241.254, 2005.

[23] ARANYOSSY, M.; NEMESLAKI, A.; FEKÓ, A. “Empirical Analyis of Public ICT Development Project Objectives in Hungary,” *International Journal of Advanced Computer Science and Applications,* vol. 5, no. 12, pp. 45-54, 2014.

[24] EUROPEAN COMMISSION, “Scoreboard 2014 - Developments in eGovernment in the EU 2014,” 28 05 2014. [Online]. Available: https://ec.europa.eu/digital-agenda/en/news/scoreboard-2014-developments-egovernment-eu-2014. [Accessed 26 11 2014].

[25] NEMESLAKI, A. “The theory of "IT-Government Alignment": Assessment of strategic fit in Hungary´s case,” in *Multi-Level (e) Governance: Is ICT a means to enhance transparency and democracy? CEE e-Dem and e-Gov Days 2016*, Vienna-Budapest, 2016.

[26] CORDELLA, A.; TEMPINI, M. “E-government and organizational change: Reappraising the role of ICT and bureaucracy in public service delivery,” *Government Information Quarterly,* vol. 32, no. 3, p. 279–286, 2015.

[27] BALTHASAR, A.; GOLOB, B.; HANSEN, H.; MÜLLER-TÖRÖK, R.; NEMESLAKI, A.; PICHLER, J.; PROSSER, A.; “Multi-Level (e) Governance: Is ICT a means to enhance transparency and democracy? CEE e-Dem and e-Gov Days 2016”, A. Balthasar, B. Golob, H. Hansen, R. Müller-Török, A. Nemeslaki, J. Pichler and A. Prosser, Eds., Vienna-Budapest: Austrian Computer Society, 2016, pp. 259-272.

[28] OCSKAY, GY. “ICT enabled cross-border governance,” in *ICT Driven Public Service Delivery: Comparative Approach Focusing on Hungary*, Budapest, National University of Public Service, 2014, pp. 123-136.

[29] RODRIGUEZ, B.; MANUEL, P.; MEIJER, A. “Smart Governance: Using Literature Review and Empirical Analysis to Build a Research Model,” *SOCIAL SCIENCE COMPUTER REVIEW ,* vol. 34, no. 6, pp. 673-692, 2016.

[30] PEE, L.; KANKANHALLI, A. “Interactions among factors influencing knowledge management in public-sector organizations: A resource-based view.,” *Governement Information Quarterly,* vol. 33, no. 1, pp. 188-199, 2016.

[31] KISILOWSKI, A.; KISILOWSKA, I. “Administrategia (in Hungarian)”, Budapest: HVG, 2017.

[32] BRYNJOLFSSON, E.; MCAFEE, A.:"The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies", New York, USA: W.W. Norton & Company, 2014.

[33] KAPLAN, R.; NORTON, D.; "The Balanced Scorecard: Translating Strategy into Action", Boston, MA: President and Fellows of Harvard College, 1996.

[34] BEKKERS, V.; "Why does e-government looks as it does? looking beyond the explanatory emptiness of the e-government concept," *Information Polity,* vol. 17, no. 3-4, p. 329–342, 2012.

[35] BÉLANGER, F.; CARTER, L. "Digitizing Government Interactions with Constituents: An Historical Review of E-Government Research in Information Systems," *Journal of the Association for Information Systems,* vol. 13, no. 5, pp. 363-394, 2012.

[36] VIRILI, F.; SORRENTINO, M. "Value generation in e-government from service-based IT integration," *Transforming Government: People, Process and Policy,* vol. 3, no. 3, pp. 227-247, 2009.

[37] NAMBISAN, S.; LYYTINEN, K.; MAJCHRZAK, A.; SONG, M. "Digital Innovation Managemement: Reinventing Innovation Management in a Digital World," *MIS Quarterly,* vol. 41, no. 1, pp. 223-238, 2017.

[38] BERTOT, J.; ESTEVEZ, E.; JANOWSKI, T. "Universal and contextualized public services: Digital public service innovation framework," *Government Information Quarterly,* vol. 33, no. 2, pp. 211-222, 2016.

[39] BARRETT, M.; DAVIDSON, E.; PRABHU, L.; VARGO, S. "Service Innovation in the Digital Age: Key Contributions and Future Directions," *MIS Quarterly,* vol. 39, no. 1, pp. 135-154, 2015.

[40] YOO, Y.; BOLAND, R.; LYYTINEN, K. MAJCHRZAK, R. "Organizing for Innovation in the Digitized World," *Organization Science,* vol. 23, no. 5, p. 1398–1408, 2012.

Workshop on Smart Cities, Council of Europe II

TOP TEN SMART CITIES IN THE WORLD. WHAT DO THEY HAVE IN COMMON AND HOW CAN EASTERN EUROPEAN CITIES USE THAT?

Catalin Vrabie[1] and Andreea-Maria Tirziu[2]

DOI: 10.24989/ocg.v331.14

Abstract

Although the smart city concept is rather old, the literature fails in defining it properly – however, most, if not all, scholars are sharing the same idea: a main characteristic of smart cities is the use of information and communications technology in all aspects of city life. All of the actors actively involved in building a smart city (and we mention here academia, IT professionals and municipalities' officials) are trying to build up a common definition, but until now they were not successful. However, many smart city rankings have been made by different researchers from various fields of activity. In this paper we will use the indicators that were found as being common in some of those rakings (made by prestigious institutions) in order to find the most common features of a smart city. Our intention is to suggest a model of a smart city based on the existing international experiences and to offer it for study to municipalities' officials in Romania and other countries in the region. The main research method will be a quantitative one (based, as we have already mentioned, on the common indicators used in building international rakings), but we will use a qualitative one as well in order to highlight, as study cases, few of the most notorious examples of smart cities.

1. Introduction

We often ask our collaborators to seek to identify the problems their city is facing, problems that, given the complexity of a locality, can be individualized and solved, partially at least, by using modern technologies specific to the information era we are living in. We want them to write down every idea that appears so that, in the design phase of a smart city, we can appeal to those ideas by also investigating the infrastructure, data and technologies already in place.

IESE insight business knowledge portal [10] – IESE is consistently ranked among the world's very best business schools [24] alongside the Business Insider portal [3] – No. 1 business publication in the United States [25], have been chosen as milestones in our analysis due to the popularity among citizens of the information disseminated through them, offer a top of the smartest cities in the world as well as some indications on how to get to that top.

Companies developing smart solutions having as a starting point the service providers, are often surprised by the fact that their products or services are not popular among government agents or citizens (unless the law requires it – such as the electronic public procurement system in Romania, SEAP/SICAP [17], but in this case the desire of users to work with the system is uncertain).

[1] Lecturer, PhD., The National University of Political Studies and Public Administration (SNSPA) – Faculty of Public Administration, Bucharest, Romania. Email: cataloi@yahoo.com

[2] PhD. candidate, The National University of Political Studies and Public Administration (SNSPA) – Faculty of Public Administration, Bucharest, Romania. Email: tirziu.andreea@yahoo.com

Developers often fail when they try to understand the real needs of users/citizens; therefore we believe that they should be involved in the strategic planning process in order to achieve successful *smart* solutions. We will further see what were the basic ingredients in developing the smartest cities in the world.

2. Overview of the smartest cities in the world (2017)

Rank	City, Country	Observations	Key elements
1	Copenhagen, Denmark	Boasts a healthy startup ecosystem, a large number of Wi-Fi hotspots, and a relatively low amount of traffic congestion. The city is also investing in clean energy, with a goal of being 100% carbon-neutral by 2025.	technology, environment
2	Singapore	Features one of the most cost-efficient public transport networks in the world [18].	mobility and transportation
3	Stockholm, Sweden	A large portion of city buses and trains run on clean fuels. Renewable power sources account for 52% of Swedish energy production.	environment, mobility and transportation
4	Zurich, Switzerland	Has an urban plan that includes a high percentage of green space.	environment
5	Boston, US	The metro area around it has several colleges, including MIT and Harvard, which lead the 2018 World University Rankings.	education
6	Tokyo, Japan	The rail system handles over 100 train lines and 14 billion passengers per year.	mobility and transportation
7	San Francisco, US	Has a high number of startups.	economy, human capital
8	Amsterdam, Netherlands	Has well-established startup communities, along with successful incubator programs like StartupDelta [19] and StartupAmsterdam [9].	economy, human capital
9	Geneva, Switzerland	Has prioritized energy-efficient infrastructure in its buildings and public transit. By 2020, the city plans to reduce its carbon dioxide emissions 21% below 2005 levels.	environment
10	Melbourne, Australia	Received a perfect score on its 4G connectivity.	technology

Table 1: Top ten smart cities in the world according to Business Insider [3]

Counting the key elements in Table 1, it is easy to observe that Business Insider considers that a smart city should have, as the most important features, the following elements:

- Environment (4) – clean energy and the presence of green spaces are among the most important aspects;
- Mobility and transportation (3) – very closely related to the environment feature; it mostly refers to the municipality's ability to build a green and efficient transportation system for its citizens;

- Technology (2) – it mostly refers to connectivity either by Wi-Fi or 4G;
- Economy (2) – the presence of a large number of startups shows the openness of the city's officials to the future;
- Human capital (2) and education (1) – it might not be visible from the table above, but all the cities mentioned are large university centers, aspect that we consider very important for the smart cities' development due to the research centers that usually operate within the universities.

Rank	City, Country	Observations	Key elements
1	New York, US	Important economic center, very well developed in terms of technology (second place on the top for this dimension).	economy, technology
2	London, UK	Best mobility and transportation and the use of human capital	mobility and transportation, human capital
3	Paris, France	The world's most popular tourist destination	tourism
4	San Francisco, US	Best economy and use of human capital	economy, human capital
5	Boston, US	Human capital and governance	human capital, governance
6	Amsterdam, Netherlands	Urban planning and technology	urban planning, technology
7	Chicago, US	Governance, economy and human capital	governance, economy, human capital
8	Seoul, South Korea	Best mobility and transportation and the use of technology	mobility and transportation, technology
9	Geneva, Switzerland	Best public management	public management
10	Sydney, Australia	Technology and to some extent public management	technology, public management

Table 2: Top ten smart cities in the world according to IESE Business School [10]

Despite the fact that only few cities are in both classifications in top ten smart cities (only San Francisco, Boston, Amsterdam and Geneva), they share the same approaches, and those are:

- Human capital (4) – being one of the most important assets, closely linked to education, it is definitely a key ingredient for building a smart city;
- Technology (4) – it mostly refers to the use of mobile apps that make citizens' life more comfortable (parking solutions, traffic congestions, incidents reporting systems etc.);
- Economy (3) and tourism (1) – being an important economic center in the country or region, these are important aspects for the smart cities' development because the public sector and the private one are working together to implement new solutions;

- Governance (2) and public management (2) – show the city's official strategic views on the future;

- Mobility and transportation (2) and urban planning (1) – as well as in the Business Insider case, IESE Business School refers to the municipality's ability to build a green and efficient transportation system.

For both tables we have taken into consideration the rakings that covers all dimensions (as in the fourth column of each table – Key elements) of urban life.

3. Best international case studies

Studying the list of smart cities in the world on both the above mentioned publications, along with their key features, we discovered interesting study cases that we consider as being important to be presented in this section of the paper mostly because they offer collaborative instruments for developing the smart cities concept – one of Romania initial priority, mostly in its commitment to assuring post-communism freedom-of-speech era, was establishing dialog frameworks [27]; therefore, the authors consider the first three international case studies as being collaborative-models-to-follow by Romanian municipalities. The next ones are examples-to-be-followed due the social innovation instruments they emphasize [26].

Reykjavík, Island, is not on the top ten lists. However it developed one of the most interactive platforms between the municipality and the citizens. **Better Reykjavík** offers citizens the opportunity to work with Reykjavík city hall. By accessing online content, they can propose, debate and vote ideas for improving city life. The best ten or fifteen of these are added to the local public administration's agenda every month, and the general city hall council is committed to processing and responding to everyone, while creating a dialogue between citizens and mayors, this being a way of elaborating local public policies. Starting in 2011 – the year of launching the platform, and until the time of drafting this paper, over a thousand ideas have been discussed by the general council of Reykjavík, of which several hundred have been accepted. To be noticed in this case is the civic engagement of the Icelandic capital's inhabitants: of the approximately 120,000 inhabitants of the city, more than 70,000 have participated in this process since the platform was launched, managing to direct over 18 million EURO towards putting their ideas into practice [4].

Figure 1: Better Reykjavík [4]

An example for Bangalore city, India, is the **NextBengaluru** platform [15] which was created independently of the city leaders by a nonprofit organization, MOD Institute [13], and aims to involve citizens in urban planning. It is a place where locals can express their ideas and requirements in accordance with the needs of the city, discuss its future, and collaborate for aligning to a common vision. From the end of 2014 to the time this article was written, the platform connected online and offline locals and managed to collect 454 ideas. At the moment, the MOD Institute tries to persuade the mayors to adopt those ideas at least partially [14].

Milton Keynes, a city in the South East England region, UK, made in 2015, as part of the MK:Smart project [12], **Our MK** platform [16]. Citizens are encouraged to send ideas that influence the community and help shape a beautiful future for the city. They, therefore, have the possibility to innovate, collaborate, share ideas, by building projects and thus changing their community. In addition, as a bonus for civic engagement, a £ 5,000 prize was set up for groups of citizens who have innovative ideas, with an important technological component, ideas that could have a strong impact on Milton Keynes city. Despite the viability of the project and the prize, the civic commitment of the inhabitants was not the one expected – only thirteen project ideas have been submitted [16]. However, we have presented the project because we find it interesting and maybe in this manner, the British example will be taken over and applied to an environment more active from this point of view.

The capital of Finland, Helsinki, promises to transform, by 2025, the current public transport system into a **mobility-on-demand** one [5]. The goal is to provide residents with a choice of cheap, flexible and coordinated options to compete with the use of personal vehicles. Officials want mobile applications specially developed for this purpose to work both as assistants in planning a trip and as payment platforms for those trips, thus enabling residents to be more efficient with their time and financial resources – users will set a starting point and a destination (similar to the Uber system [22]) as well as transport means preferences, and the application will return a plan that can combine the use of autonomous cars, buses, trains, ferries and even bicycles [21].

Bicycle riding – a very popular means of transport in Western Europe, as well as walking, can also be helped by technology. **Beat the Street** app, developed by Intelligent Health, aims to transform the city into a game where residents can earn points based on the number of steps they take, their time spent on a bicycle or running. Each user has an RFID (Radio-Frequency Identification) card with the help of which he/she identifies himself/herself in passing by beat boxes placed all over the city. From the moment in which the project was launched (2016) until now, developers boast a total of 810,710 users [1].

CycleEye app, a collision avoidance system developed by Fusion Processing, aims to alert drivers of buses, coaches and cargo carriers regarding the existence of a bicyclist in the proximity of their vehicle, thus helping to avoid an accident. The technology is based on camcorders placed outside of large-sized cars, cycling sensitive cameras – in other words, it identifies the bicyclist, with great accuracy, from the rest of the traffic participants [6].

Figure 2: CycleEye – Collision Avoidance [6]

Fusion Processing also develops applications for autonomous machines: **CAVstar** [7] – autonomous vehicle sensing and control system, as well as for traffic sensors: **TrafficTrak** [8]. Although independent, these applications can very well work together to streamline passenger transport.

4. Romania best cases

City of Brasov built up a Business Intelligence Reporting system. It was developed in order to bring together, under the same screen, all the data from every partner, contractor and sub-contractor who reports to the city hall. All this information flow is possible by an easy-to-use Graphical User Interface which allows all the actors to input data effortlessly and with accuracy [2].

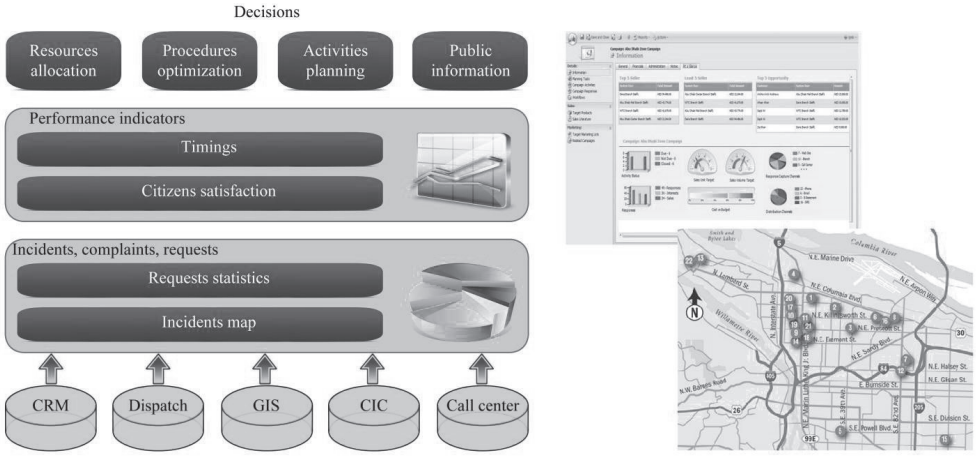

Figure 3: Business Intelligence Reporting system [2]

This site is connected to the following systems:

- Municipality video surveillance;
- Public lightning services;
- Semaphore management system along with data from specific software applications used for traffic control and management;
- The geographic subsystem – Geoportal;
- E-documents system.

Constanta municipality together with Telekom successfully tested two major smart cities solutions. The first one is for the street lightning: a large number of LED bulbs were installed, with reduced consumption and automatic dimming according to some predefined scenarios. Moreover, all of them are remotely controlled by the operators. The second *smart* solution is related to the parking issue. As a pilot project in Constanta, there are 50 parking lots that are operated by a single control panel. The user interface of the portal is also available as a mobile app and the drivers might get a notification whenever they are near a free parking lot. The intention is to size scale the project for the entire city [20].

5. Conclusions

Clearly, for a city to be smart there are no specific recipe and definitely the city officials should understand very well the city's demands. However, few things should be taken into consideration as key ingredients and those are: education, technology, mobility, environment and more, as shown in Table 1 and Table 2.

If we are to look at the Romanian best cases – in this article there were presented only two, but of course there are more, we will see that municipalities are now focusing mostly on the technology

(and mobility) features, not taking very seriously into account the education and environment features that were found so often in our top ten smart cities of the world.

We strongly believe that Romanian cities today (and maybe not only Romanian) tend to be more outsmarted than smart [11] therefore we suggest to focus more on the real needs of the citizens and the city overall.

Moreover, a city can be considered smart if its citizens are *smart*. Hence, we consider that it is important for citizens to gain access to the specific education feature needed in every smart city. Individuals should receive a proper training [23] regarding what a smart city is, how they can adapt to living in such a city and how they can get involved in the process of its development and continuity. In this case and not only, their willingness to learn is a key element because if people do not want to be a part of the information era and do not want to adapt to this new way of living, then the whole process of developing a smart city will be affected as for the many individuals are oriented in this direction, the better and easier the path to success is.

All in all we consider that a model-to-be-followed by Romanian municipalities should start from collaboration and education aiming to find the most suitable technical solution, for the local environment, that should be implemented.

6. References

[1] BEAT THE STREET, https://www.beatthestreet.me/UserPortal/Default, accessed on 12.12.2017.

[2] BRASOV CITY HALL, http://www.brasovcity.ro/, accessed on 13.12.2017.

[3] BUSINESS INSIDER, These 10 cities are the most prepared for the future, http://www.businessinsider.com/smart-cities-ranking-easypark-group-2017-11/#10-melbourne-australia-received-a-perfect-score-on-its-4g-connectivity-1, accessed on 11.12.2017 (2017).

[4] CITIZENS FOUNDATION, https://citizens.is/portfolio_page/better_reykjavik/, accessed on 11.12.2017.

[5] ENERGYCITIES, http://www.energie-cites.eu/db/Helsinki_Pocacito_Mobility-on-demand_2015_en.pdf, accessed on 12.12.2017 (2015).

[6] FUSION PROCESSING, http://www.fusionproc.com/products/, accessed on 12.12.2017.

[7] FUSION PROCESSING, http://www.fusionproc.com/cavstartm/, accessed on 12.12.2017.

[8] FUSION PROCESSING, http://www.fusionproc.com/trafficmonitor/, accessed on 12.12.2017.

[9] IAMSTERDAM, https://www.iamsterdam.com/en/business/startupamsterdam/we-are-startupamsterdam/what-is-startupamsterdam, accessed on 11.12.2017.

[10] IESE BUSINESS SCHOOL, IESE Cities in Motion Index 2017, http://www.iese.edu/research/pdfs/ST-0442-E.pdf, accessed on 11.12.2017 (2017).

[11] KISILOWSKI, M., CEE Cities: Smart or Outsmarted?, Central European University, paper presented at the Smart Cities Conference, 5th edition, December 7, 2017, SNSPA, Bucharest, Romania (2017).

[12] MK:SMART, http://www.mksmart.org/, accessed on 11.12.2017.

[13] MOD INSTITUTE, http://www.mod.org.in/, accessed on 11.12.2017.

[14] MOD INSTITUTE, About NextBengaluru, http://www.mod.org.in/mod/wp-content/uploads/2015/03/MOD-Nextbengaluru-.-PEOPLES-VISION-ON-FUTURE-SHANTHINAGAR-Booklet-_-web.pdf, accessed 11.12.2017.

[15] NEXTBENGALURU, http://gatishil.nextbangalore.com/#about, accessed on 11.12.2017.

[16] OUR MK, https://ourmk.org/, accessed on 11.12.2017.

[17] ROMANIAN DIGITAL AGENDA AGENCY, Public procurement reform – SICAP platform, https://www.aadr.ro/reforma-%C3%AEn-domeniul-achizitiilor-publice-platforma-sicap_148_0.html, accessed on 11.12.2017.

[18] SIEMENS, Singapore Climate Close-Up, https://www.siemens.com/press/pool/de/events/2014/infrastructure-cities/2014-06-CCLA/singapore-climate-close-up.pdf, accessed on 11.12.2017 (2014).

[19] STARTUPDELTA, https://www.startupdelta.org/, accessed on 11.12.2017.

[20] TELEKOM, https://www.telekom.ro/despre-noi/media/news/telekom-lanseaz-un-nou-proiect-pilot-de-tip-smart-city-n-constana/article113312, accessed on 13.12.2017.

[21] THE GUARDIAN, https://www.theguardian.com/cities/2014/jul/10/helsinki-shared-public-transport-plan-car-ownership-pointless, accessed on 12.12.2017 (2014).

[22] UBER, https://help.uber.com/h/738d1ff7-5fe0-4383-b34c-4a2480efd71e, accessed on 11.12.2017.

[23] VRABIE, C., Elements of IT for the public administration, vol. 2, 2nd Edition, Pro Universitaria Publishing House, Bucharest (2014).

[24] IESE BUSINESS SCHOOL, https://www.iese.edu/en/about-iese/rankings-accreditations/rankings accessed on 25.02.2018 (2018)

[25] BUSINESS INSIDER, http://www.businessinsider.com/business-insider-traffic-2014-11 accessed on 25.02.2018 (2014)

[26] TÎRZIU, A.M., Social innovation labs – instruments of social change, Proceedings of the "Smart Cities" Conference (SCC), 4th edition, December 8-9, 2016, Pro Universitaria Publishing House, Bucharest, Romania (2017)

[27] BERRY DAVID, The Romanian Mass Media and Cultural Development, Routledge publishing house, New York (2017)

DIGITAL GOVERNMENT AS SERVICE DELIVERY FOR DIFFICULT TERRITORY A CASE STUDY OF BONIN ISLANDS

Hiroko Kudo[1]

DOI: 10.24989/ocg.v331.15

Abstract
The paper analyses the potential of digital technology to deliver public services in difficult places to discuss the equity and equality issues of public services, through a case of Bonin Islands in Japan. It examines and discusses the issues of these difficult areas in terms of public service delivery from theoretical as well as practical aspects, and to explore the potential of digital technology, which has enabled various services and has created new opportunities.

1. Introduction

Modern nation States have promoted integration among populations and territories, while conserving and guaranteeing various diversities. European Union, for example, has been promoting integration of the member states, while guaranteeing their diversities. However the recent financial difficulties have been forcing many member states to cut their budget on these issues.

In order to examine the issue of diversity, the concept of insularity (Ottaviano, 2007) would provide an interesting view as explored in this paper. Inside a country, remote territories provide various diversities; however guaranteeing equal public services to these areas could be a big burden to the government. In case of islands territories, the benefit includes richness in climate, vegetation, and resources, as well as guaranteeing Exclusive Economic Zone (EEZ) [20]. Thus, the cost for service delivery could be compensated with the possible economic activities and the resources, produced by and in the EEZ. Even though, the austerity tendency has made the governments' investment to these areas difficult to justify and some have brought the privileges of these areas into discussion.

Some of these regions have developed excellences in public service delivery worth investigating. There are various cases which are considered to be innovative, not only because of its ICT use, but also for its ideas and challenges. Insularity seems to strengthen the local identity and favours its promotion. Previous studies show that the limited partners due to their geographical positions create positive synergies between actors and thus innovation in public service delivery; in some other cases, various founding for insularity plays an important role to create opportunities [19].

The paper analyses case of Bonin Islands in Japan, in order to examine and explore the potential of ICT, which has enabled various services and has created new opportunities. The Islands have positive impact on guaranteeing diversity to the country through their unique ecosystem, recognized as UNESCO World Natural Heritage, and wide EEZ, which produces and would produce rich aquatic and mineral resources. The territory also has significant impact on the national security.

[1] Professor, Faculty of Law, Chuo University, Higashi-nakano, Hachioji, Tokyo, 192-0393, Japan, hirokokd@tamacc.chuo-u.ac.jp

Thus, despite the high cost, it is essential to maintain the services to the inhabitants. And ICT, indeed, has proved to be an important element for the service provision.

2. Digital Governance as Alternative Public Service Delivery

Information and Communication Technology (ICT) is considered to be introduced in public administration along with other new managerial techniques, especially under the New Public Management (NPM) concept in the Nineties. With NPM, the use of ICT started to focus on managerial process of public administration. Various managerial tools enabled by ICT were introduced to improve the speed and transparency of administrative procedure. Exchange of documents and elaboration through multiple actors became easier, thus improving interaction and collaboration among stakeholders. Not only the internal managerial issues, but also the public service delivery utilizing and benefitting from ICT, especially web-based technologies became popular. Many former counter services were transformed into on-line services, making citizen possible to access directly to information as well as public services.

E-Government has been challenged with "digital era governance", which goes beyond the NPM. In this view, all stakeholders are related in public governance network. The introduction of New Public Governance (NPG) in public service delivery is an important turning point as concept as well as practice. Citizens and communities are invited to participate not only in the decision-making process, but also the service delivery process, thus realizing co-design, co-creation, and co-production. They are redesigning the structure of service delivery.

Digital services of governments have become an importance aspect of technology and/or innovation driven public services. This concept as well as practice was enabled through various elements, including co-design and co-production with citizens and other stakeholders, digital technologies enabling data analytics, thus better designing services, based on data and evidences, NPG helped the realisation of co-production with citizens and other stakeholders, while NPG encouraged ICT to be an effective and efficient instrument of government. Many of the digital services are not only a result of technological innovation and advancement, but also a product of institutional reform and revolution. ICT, per se, is not a solution, but could offer and become an opportunity.

3. Insularity and its theoretical Background

There are studies from legal, normative, economic, and territorial development points of view; the paper focuses on the insularity first from normative point of view, especially in EU context, which has developed an elaborated system on this issue, and then from New Economic Geography (NEG).

3.1. Insularity in EU Context

Ultra-peripheral regions (UPRs) and outermost regions (OMRs) have various characteristics which distinguish themselves from their main territory as well as the territory of EU. They have economic and political importance to their states as well as EU. Their diversity has considered important in contrast to the European unity. Article 299 n.2 of the Treaty of Amsterdam acknowledges that the UPRs have specific characteristics that differentiate them from other European regions. The European Council is assigned the task of designing the conditions under which the Treaty applies to those regions within the framework of the internal market and common policies.

The Treaty of Lisbon redefined the concept with OMRs. OMRs are geographic areas, which are part of an EU Member State, are situated outside of Europe and are fully part of the EU. According to the Treaty on the Functioning of the European Union, both primary and secondary EU law applies automatically to these territories, with possible derogations to take account of their "structural social and economic situation ... which is compounded by their remoteness, insularity, small size, difficult topography and climate, economic dependence on a few products, the permanence and combination of which severely restrain their development ..."[2]. As of April 2014, a total of nine territories (six French: Guyana, Guadeloupe, Martinique, Mayotte, Réunion, Saint Martin; two Portuguese: Azores and Madeira; and one Spanish: Canary Islands) were registered to have OMR status.

The task is daunting because UPRs or OMRs are "a case apart" [7]. These are regions that belong to the EU but, at the same time, also to geographical and economic areas that are not European. Not only they are far from their national mainland but they are also close to non-European countries that are much less developed. As a result, their situation is characterized by remoteness, insularity[3], small size, difficult topography, harsh climatic conditions, and strong dependence on few products [12]. OMRs have many issues due to their remoteness from major territories of EU; however thanks to the characteristics, especially of their geography and climate, they have been serving as important research fields as well as industrial hubs. They supply rum, sugar, tropical fruits and vegetables to European market and consumers, thus guaranteeing the diversity in EU. They are strategic territories for EU diplomacy with non-EU neighbouring countries.

It is important to define strategy towards OMRs by examining their specificities from economic theory. In particular, there are some key questions: has the concept of 'outermost' received any attention in economic models?; what implications those models have on OMRs?; what insight do they provide on development policies for those regions? These questions are tackled from 'New Economic Geography' (NEG), an approach to economic geography firmly grounded on recent developments in mainstream industrial organization and international trade theory.

3.2. Insularity by New Economic Geography (NEG)

According to NEG the growth opportunities of a region depend on the relative size of its local market ('market-seeking attraction'), its comparative advantage ('cost-seeking attraction') and its position in the national and international trade network ('accessibility'). These characteristics nicely fit the concept of 'outermost' according to which 'outermost' is the combination of weak attraction and bad accessibility. That is indeed what differentiates OMRs from central regions (strong attraction and good accessibility), peripheral regions (strong attraction but bad accessibility), and marginal regions (weak attraction but good accessibility) [11].

When observing geographical asymmetries in economic development, the first obvious explanation is that regions differ in terms of their relative abundance of natural resources, their proximity to natural means of communication, and their climatic conditions. All these characteristics define the exogenous attributes of a region ('first nature') and they play centre stage in traditional trade theories of comparative advantage along the lines drawn by Ricardo, Heckscher and Ohlin [5]. In particular, those theories argue that international cost differences foster the concentration of industries in countries where the corresponding costs are lower ('cost-saving attraction'). For a specific sector, these are regions that: 1) use relatively advanced technologies in the sector; 2) are

[2] Article 349 (ex Article 299(2)) of the Treaty on the Functioning of the European Union.
[3] Even 'double-insularity' as some OMRs consist of groups of islands themselves rather far from one another.

relatively abundant in the factor in which the sector is relatively intensive; 3) offer better local infrastructures for transporting intermediate goods. Nevertheless, dramatic differences in economic development can be observed even between areas that are not very different in terms of those exogenous attributes. This suggests that the observed regional unbalances must be driven by some other forces ('second nature') that are inherent to the functioning of economic interactions and that, in principle, are able to generate uneven development even across ex-ante identical places.

Second nature explanations have a long history in economics, geography, and regional science [9]. However, the debate within mainstream economics has been dominated by NEG[4]. With respect to alternative approaches, the defining feature of NEG is its focus on market rather than non-market interactions. This is pursued within a 'general equilibrium' framework stressing the endogenous determination of good and factor prices and the importance of economy-wide budget constraints[5].
This section aims to illustrate the main features of NEG. The corner stone of NEG is the location decision of the firm[6]. It is also a well-defined theoretical problem provided that the firm has some market power[7]. Increasing returns to scale at the plant level and costly transportation then generate an economic trade-off between the 'proximity' to dispersed customers and suppliers on the one hand, and the 'concentration' of production in few large plants on the other. Hence, international differences in local market size foster the agglomeration of industries in larger countries ('market-seeking attraction')[8]. The firm's location decision is made more complex by the interactions with other firms. Product and factor market competition promotes the geographical dispersion of industries ('market-crowding repulsion'). Since firms have market power, plant-level scale economies have also crucial implications in terms of welfare. The reason is that the prices, on which consumers and firms base their consumption, production and location decisions, do not fully reflect the corresponding social values. This means that market interactions generate 'side effects' for which no quid-pro-quo is paid. Being associated with market transactions those 'side effects' are called 'pecuniary externalities'. Alternative approaches to NEG stress the role of 'technological' rather than 'pecuniary' externalities[9].

Technological externalities differ from pecuniary ones in that they materialize through sheer physical proximity independently from any market transaction[10]. As they arise from non-market interactions, also for them no quid-pro-quo is paid. The productivity of a firm is influenced by the presence of other firms nearby even without any market relation with them. For instance, nearby firms may increase a firm's productivity through informal knowledge transmission ('spillover'), generated as a by-product of their contacts with the surrounding environment. The logical advantage of pecuniary externalities lies in the possibility of relating their emergence to a set of well-defined microeconomic parameters. This has proven to be quite difficult in models based on technological externalities as these still remain mostly 'black boxes'[11].

---

[4] After more than a decade since the seminal work by [17], NEG has grown into a mature body of literature as testified by a rich list of surveys and textbooks such as [30], [10], [27], [31], [32], [9], [2], [28], [29].
[5] In the words of [8]: "you want a general-equilibrium story, in which it is clear where the money comes from and where it goes".
[6] [34] explores the 'folk theorem of spatial economics'.
[7] See [35]. Firms have market power when they do not take market prices as given as perfectly competitive firms would. Under such a price-making behaviour, called 'imperfect competition', firms trade quantity against price in making their profit-maximizing decisions.
[8] This is sometimes called the 'home market effect' [16], [13], whereby firms tend to solve the trade-off between proximity and concentration by serving the smaller market from the larger one.
[9] The distinction between pecuniary and technological externalities is due to [33].
[10] [22], [14] as well as [4] for a recent reassessment.
[11] [31] as well as [6] for recent assessments.

Three possible scenarios are especially relevant for NEG. The first provides an example of market-crowding repulsion. When a firm relocates, it decreases competition in the place of origin and increases competition in the place of destination. A pecuniary externality materializes in both places in so far as the relocating firm disregards those effects. In particular, the relocating firm imposes a positive externality on its competitors in the place of origin and a negative externality on its competitors in the place of destination. By pushing down profits in places crowded by firms, competition acts as a dispersion force [32]. The second scenario is an example of market-seeking attraction and considers the effect of firm relocation when matched by labour migration. In this case, as the firm moves, it reduces demand in the place of origin while increasing it in the place of destination. As profits rise with demand, the firm imposes a negative externality on competitors in the former place and a positive one on competitors in the latter. By raising profits in places crowded by firms, market size therefore acts as an agglomeration force [17]. In the third scenario cost-saving attraction is at work. Firms are linked by input-output linkages: what is output for a firm is input for the others and vice versa. When a firm relocates, it depresses both final demand and intermediate supply in the place of origin, whereas it reinforces them in the destination. Other firms' profits suffer in the former place, where the firm imposes a negative externality, and thrive in the latter, where it imposes a positive externality. By raising profits in places crowded by firms, input-output linkages therefore act as an agglomeration force [18] [37].

The geographical distribution of demand and the position of other firms determine the relative attractiveness to a firm of alternative locations through market or non-market interactions. This creates a feedback mechanism among firms' location decisions through which firms' interactions ('second nature') may alter the economic landscape implied by natural resources, natural means of communication, and climatic conditions ('first nature'). Since 'second nature' is driven by localized externalities, in a free market the location of firms is generally inefficient and appropriate public intervention is needed.

NEG explains the public service delivery difficulties in isolated places. The following case study, however, would illustrate that the technological aspect, especially digital technology eventually can compensate the geographical distance, confirming the alternative approaches to NEG which stress the role of technological externalities.

4. Bonin Islands and their Issues

Japan is an island country with 6,852 islands of international definition. Many of them are located in coastal areas and/or in inland seas, but some are in high seas. These remote islands have suffered from low standard of infrastructure, industrial investment, and quality of public services, while their existence is extremely important for the security, natural resources, and economic activity, especially the fishing industry [20].

The government thus enacted law in 1953 to promote the territorial development of remote islands. Since then, every ten years the law have been amended and renewed until the last amendment in 2014. The law has aimed to fill the various gaps between these remote islands and the rest of the territory, investing into infrastructures like water supply and sewage system, port facility, road, and airport, improving quality of life of the residents supplying better education, healthcare and medical services [25]. These legislations have guaranteed the national investment in these territories and thus the general development. In order to guarantee equal public services in these areas, the investment is heavier than in other territories. This has been an argument and dispute from various points of view. Several islands with historical issues, including the occupation during and after the

Second World War, have their own special laws implemented through specific programmes[12]. One of them is "Special Law on Development of Ogasawara (Bonin) Islands", and was enacted first in 1969, revised and amended each 5 years. The last and current law was enacted in 2014 with various development programmes using ICT, especially digital technology. Since then, Bonin Islands saw important improvement in their infrastructure and quality of life, although the islands are located about 1,000 km south to Tokyo and the only passenger ferry runs once a week from and to Tokyo with a travelling time of 24 hours [25]. The islands were recognized as UNESCO World Natural Heritage in 2011 and had experienced a boom in tourism, also thanks to various ICT infrastructure investments which were enabled by the special law.

The research is based on primary documents, semi-structured interviews[13], field study, and direct observation of the author as a member of the Committee for the Development of Bonin Islands, under the Ministry of Land, Infrastructure, Transport, and Tourism (MLIT) from 2007 to 2017.

4.1. Bonin Islands: history, nature, and characteristics

Bonin Islands are under special laws of the MLIT, because of their historical and geographical characteristics, while they belong to Tokyo Metropolitan Government (TMG), but situated 1,000 km south of it and are constituted of around 30 islands, including the main Chichi-jima and Haha-jima, Iwo-to, and Okinotori-shima. The islands with surface of 104km^2 guarantee about the 30% of Japanese EEZ [26]. Currently 2,493 people live on the islands, compared to the maximum of 7,711 in 1944. Major economic activities are agriculture, fishery, and tourism. The Islands enjoy unique ecosystem and belongs to Oceanian realm: the only Japanese place belonging to this realm. Because of this uniqueness the islands is also named as Eastern Galápagos Islands. The Islands are the home to many unique species which can be observed only in this place.

Bonin Islands were discovered by the Japanese in the 16th Century and were internationally recognized as Japanese territory in 1876. They attracted various countries including UK, US, and Russia, and developed through various economic activities including agriculture and fishery before the Second World War. In 1944, the inhabitants were forced to evacuate in the mainland and were not allowed to return home until 1968, when the Islands returned to Japan from the United States. While Okinawa was also under the US occupation until 1972, its inhabitants continued to live on the island, inhabitants of Ogasawara were forced to leave and were not able to return for more than twenty years. This is one of the reasons why the Islands are given special status among the territories [23]. Due to this discontinuity of life and economic activities on the island and because of the need to invest in infrastructure, the government enacted Special Law for Reconstruction of Bonin Islands in 1969. The law has been revised each five years and has renamed as Special Law on Development of Bonin Island in 1979. The revision requires participation of interested parts and academia, who take part of the Committee for the Development of Bonin Islands, under MLIT.

The special law guarantees investment to maintain and renew infrastructure, to support everyday life of the inhabitants through financial aid and direct service delivery, to promote new productive activities and employment, and to launch new experiments and projects. Last amendment was in 2014 and based on the revised special law, the Ministry issued Basic Guideline of the Development

[12] Okinawa (Islands and Prefecture) has a special status, given its unique characteristics; however it is under the Cabinet Office (CAO) [3].
[13] Interviews were conducted to officials of MLIT, Ministry of Environment, and TMG, and researchers of Tokyo Metropolitan University stationed in the Island research centre.

of Bonin Islands and the TMG published Plan of the Development of Bonin Islands on the same year, in order to put the law into practice [24][36].

As a member of the Committee, which discusses the revision and evaluates the state of progress, the author observed the reality of the islands and participated in the two amendments in 2009 and 2014. During the work, the committee payed several visit to the island and regularly interviewed various actors of the islands and the related institutional actors.

4.2. Issues and policies

The major challenges of the islands are; transportation from mainland, thus the general high cost of life, including energy cost and other indispensables, limited stock of goods, limited delivery service, healthcare services and medical attention, education, communication, broadcasting, internet, and maintenance and renewal of infrastructure [23] [24].

The inhabitants' life is strongly bound to the schedule of the cargo line, which has limited trip and capacity. Thus in case of extremely bad weather like Typhoon, which can stop the trip of the ship for days, the daily necessities of the inhabitants and the tourists would be lacking[14]. All types of delivery are also bound to the only ship. This means that the shipment of products such as fruits, vegetables, and fishes is also strongly dependent on it. Thus, not only the cost, but also the time and schedule of the transportation affect the economy. Construction of an airport has been one of the biggest issues, thus the topic of the special laws and the development plans; however, because of technical difficulties and environmental issues, it has not yet realised so far[15].

In order to guarantee equity and equality of public services, for example, the difference of energy cost from the national average is financed by the TMG and the higher cost of broadcasting is covered by the NHK, or Japan Broadcasting Corporation, and other private broadcasting company, as the broadcasting law requires the ubiquitous service to all territories. For the telecommunication services, after the privatization of national telecommunication company, the investment in the area has been small and always in delay compared to the rest of the territory. The services and companies operating in the territory have been limited, limiting the choice for the inhabitants.

Healthcare and educations are the most serious issues of the inhabitants, who are ageing on one hand, and who are giving more birth than other areas [26]. Patients with serious health condition which requires special medical attention have to be transported to mainland by Japan Coast Guard and Self Defence Force and expecting mothers have to deliver their baby in mainland. When it comes to education, there are elementary and secondary schools as well as a public high school, but students have to leave the islands to go to universities.

Maintenance and renewal of major infrastructure are a big issue for the Ministry and for the TMG. Major infrastructures, such as port and harbour, water purification plant, water supply and sewerage services, schools, affordable housings and clinic were built before the war or in the Sixties in a precarious way, and need to be renewed [23], but the cost of construction is extremely high, since

[14] During the summer of 2015, several big Typhoons hit the area and caused serious problems for the inhabitants of the Island and the tourists.
[15] Under the last development plan of 2014, environmental assessment and inhabitants' questioner were conducted in 2016.

every single piece of materials should be transported from outside[16]. There is also an urgent need to prepare for a possible big earthquake [23] and many old infrastructures needs anti-seismic intervention, which requires big investment as well as solving various practical issues.

The new challenges since the recognition of UNESCO World Natural Heritage are; the increasing tourists, lack of facilities and personnel, and environmental protection of the territory. The tourism industry is one of the major industry, thus the increasing number of tourist should be a positive sign; however because of the limited facilities and personnel, many of the tourists cannot be accommodated. Maintaining a unique ecosystem needs constant research, observation, management, and intervention, if necessary.

The Islands unique ecosystem with unique vegetation, habitat, and climate, has attracted international research community. The Ministry of Environment and the TMG with its Tokyo Metropolitan University have been investing to create world class research centre on the Islands. The centre has established a certain reputation on marine tropical vegetation research, climate research, and aquatic and mineral resource researches.

Various projects have been implemented according to the special laws and the development plans of the Ministry and TMG with their respective budget. Since the last special law was enacted in 2014, the major issue of the implementation of the plan has been the finance.

5. Digital Technologies and Co-production

Since the aim of the paper is to explore role of ICT, proved to be useful in improving services, the last part investigates what have been done and what are the future plans in various sectors.

Since the cost of transportation is the major financial burden for many other issues, ICT, especially digital technologies and satellite communication have been proving efficient. The government invested in the satellite communication in the area with some experiments of Japan Aerospace Exploration Agency (JAXA), and it has been widely used for telecommunication and broadcasting. For the internet services, the Islands are connected with broad band internet using optical fibre cable installed below the sea since 2011. More stable and cheaper communication has improved agriculture and fishery business, which relies heavily on the mainland market. Use of digital technologies have improved productivities of fruits and vegetables, but also in fishery business, which now operates with much technologically advances ships than it used to. The treatment and processing of fishes on the ship and at the port before the final products get shipped use market data, including price and demand. Thus the amount of catch and the excess would be under control.

Tomato is indeed one of the major agricultural products of the Islands which have an important market in mainland. Before the market analysis enabled by the mobile devices and big data, many farmers did not control their production and thus the price could have varied according to the market condition or could not simply meet the market demand. Now they control much better the production according to the demand of the market and ship their product when it is competitive.

This applies to passion fruit, acerola, and mango as well.

[16] Construction of infrastructure such as water purification plant requires transportation of not only all necessary components, but also construction equipment as well as workers, who should stay on the Islands during the period of construction.

Healthcare services are also benefitting from the digital technology. The first has been introducing telemedicine and several smartphone applications, which check and control health conditions. The inhabitants are encouraged to use them, which have been serving as preventive healthcare. Since the medical personnel are limited, the medical service on the Islands is not ready to operate using remote operation system, but the facility can accommodate a series of operation.

Faster and stable internet connection has enabled remote work and study. As a consequence, the Islands have been registering impressively high rate of newly transferred residents in recent years. For example, in 2014, the Islands registered 11.2% new residents coming from outside and 2.3% natural increase, while the national average was 4.4% and 0.2% [25]. This means that the Islands have been attracting young peoples, who settled in the area, started their activities, formed family and gave birth. This has accelerated with the recognition as UNESCO World Natural Heritage and the tourism boom, but the technology has surely supported the movement.

Communication infrastructure with Massive Open Online Course (MOOC) have been helping young inhabitants to opt not leave the Islands, or at least continue a part of their higher education remotely. On this regards, the statistical data so far shows mix results, also because of the limited number of students of that age and thus it is not easy to draw conclusions. However the number of Twenty-somethings returning to the Islands after the higher education outside the Islands could show a positive trend. Number of activities started by young entrepreneurs is also increasing, according to the TMG statistics. Given the limited number, it might be misleading to stress the relationship, but it is possible to note the trend.

Lastly, an interesting field to be noted is the weather forecasting and natural disaster prevention. The Islands, despite the importance for its climate issues, contradictory, never had the proper weather station, but relied on various nearby facilities. On this regard, there have been discussions to build a proper weather station so that the Islands can become an important hub for the climate issue as well as natural disaster prevention issue. The same reason applicable for the renewal and new building of infrastructure, the option to build a new weather station on the Islands seem financially difficult, while they decided to continue to rely on a network of facilities which gather and provide data enough to analyse the micro situation of the Islands. Some of them are even private and commercial facilities. This reminds us of the service of Japan Meteorological Agency (JMA) during and after the East Japan Earthquake in 2011, when the major data came from a network of private, commercial, research institutions, even from international partners, along from the public structure [1]. The weather related data, indeed, can be gathered by various types of institutions, but easily assembled and analysed for a certain purpose, in some cases, could be vital to prevent disaster and to rescue people and property in the best and fastest way. This is a typical benefit of co-production of, and through, Big Data [21].

6. Conclusion: Findings and limitations

This paper aims to explore a particular case of unique territorial characteristics and analyse the potentials of digital technologies through the Japanese Islands of Bonin. Thus, the findings from the case have the strength of being realistic as well as authentic; however there are also limitations of being a single case study as well as because of limited period of observation.

When it comes to potentials of digital technologies in geographically difficult places, such as remote places from cities, mountains, forests, deserts, and places with extreme climate conditions, there are many researches and publications which studies about it and proved it. Indeed, many

developing countries in Africa, South and Central Asia, and South America are benefitting from these technologies, especially in agriculture, finance, and basic citizen services [15].

Several direct findings from the case of Bonin Islands are that the Islands have been benefited from latest mobile communication technologies as well as general ICT advancement in various fields. Installation of optical fibre cables enabled stable and reliable connections, which improved various services on the Islands as well as productions, especially given the difficulties to improve transportation means and thus the cost of various services. Many indicators show that the new services have had positive impacts on the Islands and the inhabitants of the Islands.

Interviews revealed that there are several issues such as capacity development on ICT among the young inhabitants as well as the elderly population of the Islands and the rather high maintenance cost of equipment on the Islands, if it would not be done locally. There are also limitations of these technologies, as they can improve several services, but would not resolve the problem of physical transportation of materials by cargo lines or airplanes.

As one of the original issues of the insularity has been the equity and equality issue, ICT has proved to be useful and accommodated the financial issues behind it. Thus, the possible potential of ICT could be on this point. Furthermore, several services provided through co-production of various actors using Big Data have proved to be quite efficient as well as effective as the case of JMA.

The results the case study contribute also to theoretical discussions, as they show that physical distance is not the only determinant and the absolute burden as illustrated in NEG, as the digital technology might compensate geographical distance element. The case contributes to the co-production of public service delivery discussion as well, since it is an example of it.

Given the limitation of one case study, the further research which will follow would be on several other cases, and on various other technologies, including use of Big Data and IoT.

7. References

[1] ALFORD, J. and O'FLYNN, J. (2012), *Rethinking Public Service Delivery: Managing with External Providers*, Palgrave Macmillan.

[2] BALDWIN, R., MARTIN, P., and OTTAVIANO, G. (2001), "Global income divergence, trade and industrialization: The geography of growth take-off", *Journal of Economic Growth*, 5-37.

[3] Cabinet Office (CAO) (2017), *Okinawa Development Plans* (in Japanese)

[4] CICCONE, A. and HALL R. (1996), "Productivity and the density of economic activity", *American Economic Review*, 87, 54-70.

[5] CRONON, W. (1991), *Nature's Megalopolis: Chicago and the Great West*, Norton, New York.

[6] DURANTON, G. and PUGA, D. (2004), "Micro-foundations of urban agglomeration economies", in Henderson V. and J.-F. Thisse, *Handbook of Regional and Urban Economics*, vol. 4, Elsevier, Amsterdam.

[7] EURISLES (2002) "Off the coast of Europe: European construction and the problem of the islands", Islands Commission of CPMR.

[8] FUJITA, M. and KRUGMAN, P. (2004), "The new economic geography: Past, present and future", *Papers in Regional Science*, 83, 139-164.

[9] FUJITA, M. and THISSE, J.-F. (2002), *Economics of Agglomeration: Cities, Industrial Location and Regional Growth*, Cambridge University Press, Cambridge.

[10] FUJITA, M., KRUGMAN, P. and VENABLES, A. (1999), *The Spatial Economy: Cities, Regions and International Trade*, MIT Press, Cambridge, Massachusetts.

[11] FORTUNA, M., DENTINHO, T. and VIEIRA, J. (2001), "The costs of peripherality", European Parliament, Directorate-General for Research, Regional Policy Series, Working Paper REGI 111 EN.

[12] Fundo de Maneio (2006), "MACRORUP", Report elaborated in order to support experts' work, mimeo.

[13] HELPMAN, E. and KRUGMAN, P. (1985), *Market Structure and Foreign Trade*, MIT Press, Cambridge, Massachusetts.

[14] HENDERSON, V. (1978), *Economic Theory and the Cities*, Academic Press, London.

[15] ICEGOV (2017), *Proceeding; Doctoral Colloquium*

[16] KRUGMAN, P. (1980), "Scale economies, product differentiation and the pattern of trade", *American Economic Review*, 70, 950-959.

[17] KRUGMAN, P. (1991) "Increasing returns and economic geography", *Journal of Political Economy*, 99, 483-499.

[18] KRUGMAN, P. and VENABLES, A. (1995), "Globalization and the inequality of nations", *Quarterly Journal of Economics*, 110, 857-880.

[19] KUDO, H. (2013), "Public Sector Management Innovation in Special Autonomous Regions in Italy: intergovernmental relationship and public service delivery", in du Boys C., Fouchet R., and B. Tiberghien (eds.), *Management Public Durable: dialogue autour de la Méditerranée*, Bruylant, Bruxelles.

[20] KUDO, H. (2015), "Guaranteeing Diversity while Promoting Integration: Territorial, Cultural and Institutional Identities under Insularity and Multi-level Governance", in Alexander Balthasar und Klemens Fischer (eds.), *Multi-level Governance – from local communities to a true European community, Proceedings of the Conference on European Democracy 2014 (EuDEM 2014)*, Klein Publishing GmbH, Intersentia, Berliner Wissenschafts-Verlag, pp.151-172.

[21] KUDO, H. (2016), "Co-design, Co-creation, and Co-production of Smart Mobility System", in Rau, Pei-Luen Patrick (Ed.), *8th International Conference, Cross-Cultural Design 2016,*

HCI International 2016, pp.551-562.

[22] MARSHALL, A. (1890), *Principles of Economics*, Macmillan, London.

[23] Ministry of Land, Infrastructure, Transport and Tourism (MLIT) (2014a), *Amendments of Special Law on Development of Bonin Islands* (in Japanese)

[24] Ministry of Land, Infrastructure, Transport and Tourism (MLIT) (2014b), *Basic Guideline of the Development of Bonin Islands* (in Japanese)

[25] Ministry of Land, Infrastructure, Transport and Tourism (MLIT) (2016), Materials of the Committee for the Development of Bonin Islands (in Japanese)

[26] Ministry of Land, Infrastructure, Transport and Tourism (MLIT) (2017), *About Bonin Islands* (in Japanese)

[27] NEARY, P. (2001), "Of hype and hyperbolas: Introducing the new economic geography", *Journal of Economic Literature*, 39, 536-561.

[28] OTTAVIANO, G. (2003), "Regional policy in the global economy: Insights from New Economic Geography", *Regional Studies*, 37, 665-674.

[29] OTTAVIANO, G., PINELLI, D. (2005), "A 'new economic geography' perspective on globalization", *Italian Journal of Regional Science*, 4, 71-106.

[30] OTTAVIANO, G., PUGA, D. (1998), "Agglomeration in the global economy: A survey of the 'new economic geography'", *World Economy*, 21, 707-731.

[31] OTTAVIANO, G. and THISSE J.-F. (2001), "On economic geography in economic theory: increasing returns and pecuniary externalities", *Journal of Economic Geography*, 1, 153-179.

[32] OTTAVIANO, G. and THISSE, J.-F. (2004), "Agglomeration and economic geography", in Henderson V. and J.-F. Thisse, *Handbook of Regional and Urban Economics*, vol. 4, Elsevier, Amsterdam.

[33] SCITOVSKY, T. (1954), "Two concepts of external economies", *Journal of Political Economy*, 62, 143-151.

[34] SCOTCHMER, S. and THISSE, J.-F. (1992), "Space and competition: a puzzle", *Annals of Regional Science*, 26, 269-286.

[35] STARRETT, D. (1978) "Market allocations of location choice in a model with free mobility", *Journal of Economic Theory*, 17, 21-37.

[36] Tokyo Metropolitan Government (TMG) (2014), *Plan of the Development of Bonin Islands* (in Japanese)

[37] VENABLES, A. (1996), "Equilibrium locations of vertically linked industries", *International Economic Review*, 37, 341-359.

WHAT THE SMART CITY IN THE DANUBE REGION CAN LEARN FROM INDUSTRY 4.0

Alexander Prosser[1]

DOI: 10.24989/ocg.v331.16

Abstract

The Smart City Concept throughout all its current definitions is essentially a system that uses state-of-the-art ICT to provide and process information, to adapt and learn. The Internet of Things and advances in affordable sensor technology play an additional important role. The net result of the "smartification" of a city is the creation of a living, networked system of assets, devices and infrastructure. This living system continuously collects data that enables the system to learn and evolve.

This is nothing new or path-breaking. In logistics and the manufacturing industry, this concept has been widely implemented to optimise supply chains, from predictive maintenance, to dynamic route optimisation and online business intelligence (BI). "Industry 4.0" has evolved from a buzzword to everyday reality. Moreover, these technologies do not just "electrify" existing processes – they enable new processes and beyond that even completely new business models that would not have been feasible with the pre-Industry-4.0 technology. Particularly the advent of in-memory business analytics that enables BI from the original transaction data in an on-demand/online fashion has facilitated this development. Now, the public sector is discovering these technologies for its own purposes.

This contribution attempts to show the parallelism, but also differences between smart cities and Industry 4.0, where learning effects may occur and known pitfalls may be avoided.

1. Introduction

1.1. Smart City

As with any new concept, the term Smart City has been interpreted in different ways. Some place more emphasis on inclusiveness and social openness [1], environmental and sustainability aspects may play an important role [2] and others focus on technological and energy efficiency and an "intelligent" infrastructure (cf. [4] and the definition of the Wiener Stadtwerke in [3]).[2] The perhaps most widely-used definition by Frost and Sullivan encompasses "smart energy, smart building, smart mobility, smart healthcare, smart infrastructure, smart technology, smart governance, smart education, smart citizen." [5] What these definitions seem to have in common on the technological level are:

[1] University of Economics and Business, Vienna, Welthandelsplatz 1, A-1020 Wien

[2] An extensive overview of various definitions is provided by the Smart Cities Council at https://smartcitiescouncil.com/smart-cities-information-center/definitions-and-overviews

- The "smartification" of hitherto analogous infrastructure (particularly the "sensorisation of things", cf. [5]);
- Extensive use of ICT, particularly mobile services;
- The efficient use of resources on all levels (from staff to energy) due to intelligent adaptation of services and a focus on sustainability.

1.2. Industry 4.0

One has to be aware that this originally was a concept advanced in Germany [6], but has gained wide-spread usage in Europe, including the Danube Region – however, not without criticism of the terminology (for example [7]). This paper holds that, essentially, Industry 4.0 hinges on some distinct technological developments:

1.2.1. Cheap and Connected Sensors

The price of sensors in general and Internet-capable sensors in particularly has come down considerably. This is the commercial/technological driver of the Internet of Things (IoT). Image sensors and accelerometers on average have come down from 22 USD apiece in 1992 to 1.40 USD in 2014 (not inflation-adjusted) [8]. Goldman/Sachs estimates that the "average IoT sensor" has come down from 1.30 USD in 2004 to below 0.50 in 2018 [9]. Micro-mechanical devices (MEMS) have come down in prices from an average of approx. 3.50 USD in 2000 to below 1 USD in 2014.[10]

All these figures show a marked decrease in sensor/IoT element prices, which makes it economically viable to put a sensor behind any interesting part and to connect it to the Internet. An example would be Predictive Maintenance, where spare parts in investment goods (eg, large machinery) are monitored by IoT-connected sensors and when a threshold value of wear and tear is reached, a requirement is sent back to the logistics monitoring application. [11] This enables to minimise (ideally cut altogether) the spare part storage on site and yet to reach a near-ideal service level of the spare parts for the machinery (for a simulation study, see [12]).

1.2.2. Cloud Services

"The Cloud" has become yet another buzzword in enterprise computing used in many contexts, however, there is a sound technological core behind it in the context of Industry 4.0. The concept requires IoT connected modules to interact with a number of applications. Two or three decades ago this would have required enormous interface programming effort that would have stymied any commercial viability. Web services, that is SOAP-based [13] application services, enabled an object-oriented encapsulation of complete services including data storage and business logic. These encapsulated modules "export" a standardised interface in XML notation that can be "consumed" by any authorised application, whereby the latter does not need to know any details of the internal structures of the application. The web service interface, its services and expected responses are the only thing a service consumer needs to know.

This enables, for instance, a central logistics application to export a web service for reporting sensor values that (schematically) would look like the following:

```
<ID of reporter>Machine 123.456</ID of reporter>
<Value> (may appear an arbitrary number of times)
        <SensorID>123.456.1</SensorID >
        <SensorType>Accelerometer</SensorType >
        <Timestamp>4.1.2018-10:23:30-CET</Timestamp>
        <SensorValue>5</SensorValue>
</Value>
```

The only things required are (i) security and authentication procedures and parameters and (ii) semantics, eg, that an accelerometer reports values to be interpreted as m/s^2.

Web services also help to bridge gaps between different platforms and to integrate new platforms in existing applications. It is the standardised web service architecture that completely abstracts from the internals of an application which has enabled the free flow of information among application boundaries.

1.2.3. Real-Time Business Intelligence

Every transactional/operational information system is essentially a huge data-generating machine collecting formatted or unformatted digital or analogous data depending on the field of application. This can be a main source of information – providing the data stream is analysed, ideally in real time. Typical methods of analysis are multi-variate statistical methods, such as clustering, log-linear/logit models, conjoint analysis or multi-variate regression (for an introduction, see [11]). These methods, however, have one main disadvantage: They require access to the raw (transactional) data, not just to aggregates.

"Classical" business intelligence has been based on data warehouses, which are essentially multi-dimensional aggregation hierarchies.[14] Within them, analyses are easy and flexible, typically supported by graphical data modelling and reporting tools. Data warehousing typically does not go for the raw transactional data – and for a very simple reason: The amount of data would be so big that any timely analysis would only be possible for comparatively small data sets.

It is another technical innovation that has overcome the limitations of data warehouses, the steep performance increase and price drop in main memory elements.[3] This enables huge data banks being loaded into main memory. This makes a difference in access speed. The access time of a hard disk drive is measured in milliseconds (ms)[4], the access time of main memory banks in nanoseconds (ns)[5]. The difference between 1 ms and 1 ns is 10^{-6}; this means that a read operation that takes 11.5 days reading data from disk can be done in 1 second reading data from main memory.[6] Concerning capacity, standardised solutions are on the market offering 64 TB of main memory. [7] This can hold very large data banks, where the raw data can be analysed in real or near-real time without having to build inflexible aggregation hierarchies that only allow fast access to aggregate analyses like in a

[3] Just as a flashlight: In 2007, a 2x 1GB DIMM DDR2 would have been at USD 130.- (or 6.6 ct per MB); in 2017 a 2x 16GB DIMM DDR4 was at USD 185.- or 0.6 ct per MB. Source: http://jcmit.net/memoryprice.htm

[4] For an example with explanations, see http://fibrevillage.com/storage/596-hard-drive-performance-in-detail-transfer-rates-latency-and-seek-times

[5] Cf. an overview of typical elements in https://en.wikipedia.org/wiki/DDR4_SDRAM

[6] Caveat: This is a schematic and illustrative example only!

[7] For an example, see http://e.huawei.com/en/solutions/business-needs/data-center/sap-hana/tdi

data warehouse. In-memory computing offers real-time business intelligence based on unaggregated raw data.

The impact of this development on Business Intelligence cannot be overestimated.

2. Commonalities

The following sections will describe a number of commonalities between the two concepts.

2.1. Efficiency Gains through a "Living" Infrastructure

An infrastructure that is "wired" the way described Sections 1.2.1 and 1.2.2 can be constantly monitored and also returns data for optimisation which can be fed back in an optimisation loop, much the same way as MES (Manufacturing Execution Systems, for an introduction, see [15]). This optimisation loop in MES was not the original intention or focus of MES, which were originally considered the hinge between machine/infrastructure control systems (SCADA [17], cf. M1, M2, … in Figure 1) and the planning system, typically an Enterprise Resource System (ERP). MES would assign the infrastructure, load and lock orders on the machinery and confirm execution or production order steps. It would hence enable tracking and tracing of production orders and connect the ERP system to the physical machine control.

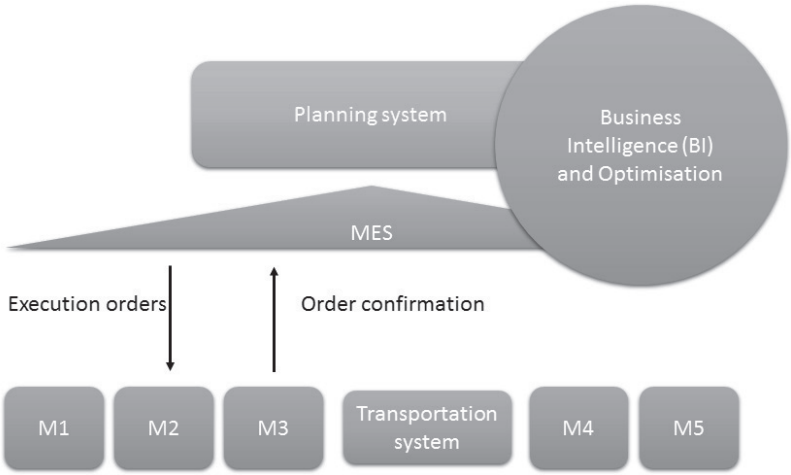

Figure 1: MES

However, the feedback of state data from the SCADA can be fed into a BI application, which then enables analyses, from a simple search for inefficiencies to the complete optimisation of the process. It can also serve as benchmarking device between comparable production facilities or to detect systematic deficiencies in production processes. Therefore, "optimisation" does not only mean optimised operational processes for, for instance, increasing machine utilisation, but also tactical optimisation by spotting and eliminating systematic deficiencies in the production process. In this context, MES have evolved into a massive data collection engine from the physical machine and transportation infrastructure that can feed its data into real-time BI. These applications are not a distant future but already in place in well-run production facilities.

This can also be done in the Smart City; consider a simple example application intended to show the potential:

(i) Equip every available free parking spot with a sensor showing, whether it is occupied or not;

(ii) Link these sensors to a central monitoring application;

(iii) Include occupation states of parking houses, which can address the application via a cloud service;

(iv) Make the current state available to motorists via smartphone app;

(v) Provide an interface to navigation apps.

This application would correspond to what is already in place, for instance in the City of Dubrovnik [18]. It leverages a "living" infrastructure, connected via the IoT and made available via a Web-based/Smartphone app-based service.

However, this feedback loop from the infrastructure also delivers a massive data base on parking utilisation, not only in very general terms as with a simple m-parking system[8], where only the total number of parking tickets is available, but down to the detailed geographical distribution of the parking usage over time. This massive data base can then be used for several optimisation purposes, such as

(i) Time distribution of the parking situation in districts and general guidance to motorists;

(ii) Real-time parking guidance via digital signposts;

(iii) Dynamic pricing of parking slots;

(iv) (Where in place,) Dynamic adaptation of city toll system.

Such applications require all elements listed in Section 1.2: IoT-enabled sensor-equipped ("living") infrastructure, cloud services and real-time BI. The applications range from isolated optimisation tolls, such as the one described to full-fledged city-wide traffic management, such as the one used in Singapore [21].

2.2. Predictive Tools

This learning process on the behaviour and determinants of the infrastructure can also be used to predict events in the physical infrastructure. A very popular example in the manufacturing industry is predictive maintenance. "Classical" maintenance schemes are either purely corrective (ie, the machine is repaired when it fails) or preventive (ie, regular maintenance activities according to the schedule prescribed by the manufacturer). The first incurs a potentially huge downtime of the machinery, the second is essentially wasteful as it tends to discard spares simply because the schedule prescribes their replacement and not because they really need to be replaced. [19] The

[8] Such as the one in place in Vienna, http://handyparken.at

issue or corrective maintenance is aggravated by long-haul supply chains, where for instance the machine producer is located in the Danube Region and the machine is used in South Asia. Buffer stocks either in situ or with local/regional supply centers may alleviate the duration of the logistics chain, but still incur capital being bound in spare stocks. [20]

The "sensorisation" of the machinery and its connection to the IoT enables to query/get information (both a pull or push model are possible); whenever a threshold value is reached by a spare part, a logistics requirement is issued to a central logistics application via a cloud service, typically implemented as described in Section 1.2.2. The threshold value is configurable and will be a lot earlier in the deterioration of the part when the logistics chain is long and with a lot of variance in duration, vice versa. When the threshold value is reached and the replenishment order issued, the part itself is still functioning perfectly – it is just time to think about a replacement. To meaningfully set the threshold value data gathering and analysis from BI applications can be used plus simulation techniques. Results show that by judiciously setting the threshold for the replenishment order a service level can be reached that corresponds to almost the service level of a (hypothetical) case, where all spares are available on site (for an example with city infrastructure, see [12]).

It is immediately obvious how the Smart City may benefit from predictive schemes; whether it is infrastructure maintenance, vehicle and machine availability or the prediction of infrastructure or device utilisation, the opportunities offered by monitoring and analysing device behaviour are essential.

2.3. New Business Models

The ability to remotely monitor a device and its usage offers completely new business models. When integrated information systems appeared in the 1990-ies on a large scale, it was – and of course still is – common sense not just to use them to "electrify" existing processes, but to use system integration to support new processes in the organisation [22, 23]. Since observation of remote devices becomes possible via IoT-enabled sensors and cloud services, one may advance the refutable hypothesis that these technologies tend to enable a movement away from ownership to pay-per-use models: *The device, the machine, the complete infrastructure as a service*.

The Smart City may benefit from this development from several angles:

(i) As a customer renting devices on a pay-per-use base rather than buying ownership of the device.

The effects on capital requirements are obvious and would be a driver very similar to the private sector, particularly in times of high sovereign debt and debt ceilings, such as those of the Euro Zone. Here careful design of the contracts may be recommended, as of course the partner renting out the infrastructure will typically set a certain minimum payable usage of the device. This may be alleviated by shared devices, particularly in the case of smaller cities. Generally these pay-per-use models are slowly gaining traction in the private sector, however, also the municipal, or in general public, administration may substantially benefit from such arrangements.

(ii) As the instance letting the devices/infrastructure elements.

Car/bike sharing models clearly belong to this model, where IoT services enable tracking of the vehicles as well as per-use payment models.

(iii) As a mediator platform.

Citizens may offer standardised or non-standardised goods in exchange for "payment" in kind; examples could be giving up one's reserved resident parking lot in exchange for a resident parking lot in another city, where municipalities provide a match-making platform. Of course, the private sector is already far ahead here with platforms, such as Uber or Airbnb – sometimes much to the chagrin of city (and tax) administrations.

3. The Main Concern: Security

As has been demonstrated in the past sections, there are opportunities and potential efficiency gains by introducing Industry 4.0 techniques into the Smart City. However, this will open the municipal infrastructure also to the very same security issues that also exist with the private sector – in some cases, such as the power grid, with even more damage potential. The private sector appears to have grasped the risk exposure and implementing IoT and cloud security have become major concerns of Industry 4.0 users. This concerns (i) the integrity of the distributed systems and (ii) the data communications between the distributed, IoT-driven data banks and central (cloud) applications collecting and analysing the data (for an introduction, see [24, 25]). Apart from that, general risks of any ICT application, such as Denial of Service Attacks, apply.

The fundamental issue with IoT-enabled and intelligent infrastructure/devices is that these devices are still produced by traditional manufacturers that have little experience with ICT. Particularly the following issues can be identified:

(i) Hardening of external interfaces, such as SOAP services [13];

(ii) Judicious use of standard tools, such as TLS (SSL) [26];

(iii) A regular process for producing and distributing upgrades and patches to the IoT devices;

(iv) Upgrades and patches to the operating system and system components used;

(v) Usage of a virus scanner;

(vi) At times, the most basic elements of systems operations are not heeded, such as enforcement of password resets.

The risk is clearly identified and concerns two areas:

(i) The smart infrastructure may be used as an entrance to backend systems, this particularly applies to the power grid;

(ii) The smart infrastructure may be used for all sorts of criminal and illicit activities.[9]

Many of these issues can be resolved by simply adopting standard ICT practices also to the world of smart devices, others may only be resolved by requesting a security certification. If devices are

[9] As an example: For some scenarios of using a smart refrigerator for terrorist activities, see https://www.wu.ac.at/en/evoting/news-details/detail/eudem-2016/

critical, such as smart meters potentially opening the path to the power grid, it would seem indicated to request Common Criteria certification [27].

However, such certification would be costly and time-consuming depending on the assurance level required (ie, the stringency of the tests) and will probably only be realised if mandatorily requested by standards set on a European level. Examples show however, that such assurance is sorely needed [28, 29].

4. The Danube Region

These considerations of course apply universally. However, things are aggravated in the Danube Region due to the fragmented character of the Region. Since the markets are too small to justify adaptation to national regulations, only supranational regulations may have the necessary effect. The security certifications discussed in Section 3, for example, can only realistically be implemented on an EU level, national regulations would fail due to small market size.

Bringing this topic on the EU agenda and not attempting purely national solutions is therefore in the well-understood interest particularly of the countries in the Danube Region.

5. Summary

The past paragraphs outlined the huge potential in the Smart City concept, its parallelism to Industry 4.0 and the technological developments underlying both. Industry 4.0 involves huge productivity gains in the manufacturing industry, there is no doubt that similar benefits may be reaped by public administration, particularly on the municipal level. Also, the technology enables completely new business models and a completely new view on the physical products of a manufacturer. The main development here is the movement from the device as a product to the device as a service – a development that has already been seen in the software industry in the past decade [30].

However, there are also differences:

(i) The driver in the manufacturing industry is mainly efficiency gains – which may of course also involve a more sustainably and more environmentally friendly way of production, customer satisfaction is a main driver, yet only one of many factors; the Smart City driver on the other hand is primarily citizen/business satisfaction and the improvement of the competitiveness of the city as a location;

(ii) Manufacturing applications of IoT and Cloud Services seldom involve personal data; if they do, a work council agreement may be drafted to enable processing of such data depending on the legal situation of the country in question; in the city context many applications will involve personal data from citizens/consumers, whereby in many cases, the data collection and processing will be “public”, ie based on sensors in the public sphere, where people cannot escape the processing; this involves additional thought, particularly under the conditions of the General Data Protection Regulation, which will soon be in effect.

6. References

[1] BEINROTT, V., Bürgerorientierte Smart City – Potentiale und Herausforderungen, Zeppelin Universität Friedrichshafen, Friedrichshafen, 2015, download from https://www.zu.de/institute/togi/assets/pdf/TOGI-150302-TOGI-Band-12-Beinrott-Buergerorientierte-SmartCity-V1.pdf.

[2] NEIROTTI, P. DE MARCO, A., CAGLIANO, A.C., MANGANO, G., SCORRANO, F., Current trends in Smart City initiatives: Some stylised facts, Cities, 38(2014), pp. 25-36.

[3] ROHDE F., LOEW, T., Smart City - Begriff, Charakteristika und Beispiele , Wiener Stadtwerke Holding AG, City of Vienna, 2011, download from http://www.nachhaltigkeit.wienerstadtwerke.at/fileadmin/user_upload/Downloadbereich/WSTW2011_Smart_City-Begriff_Charakteristika_und_Beispiele.pdf

[4] KOMNINOS, N., What makes cities intelligent?, in Deakin, M., Smart Cities: Governing, Modelling and Analysing the Transition, Taylor and Francis, 2013.

[5] FROST & SULLIVAN, Global Smart Cities market to reach US$1.56 trillion by 2020, 2014, at https://ww2.frost.com/news/press-releases/frost-sullivan-global-smart-cities-market-reach-us156-trillion-2020

[6] SPATH, D. (ED.), GANSCHAR, O., GERLACH, S., HÄMMERLE, M., KRAUSE, T., SCHLUND, S.: Produktionsarbeit der Zukunft – Industrie 4.0, Fraunhofer IAO, 2013, download from https://www.iao.fraunhofer.de/images/iao-news/produktionsarbeit-der-zukunft.pdf

[7] GARBEE, E., This is not the fourth industrial revolution, at http://www.slate.com/articles/technology/future_tense/2016/01/the_world_economic_forum_is_wrong_this_isn_t_the_fourth_industrial_revolution.html

[8] HOLDOWSKY, J., MAHTO, M., RAYNOR, M.E., COTTELEER, M., Inside the Internet of Things (IOT), Deloitte, 2015, download from https://www2.deloitte.com/insights/us/en/focus/internet-of-things/iot-primer-iot-technologies-applications.html

[9] GOLDMAN/SACHS, The average cost of IoT sensors is falling, download from https://www.theatlas.com/charts/BJsmCFAl , 2016.

[10] PIZZAGALLI, A., Mems and sensors packaging technology and trends, Presentation at Semicon West, 2016, download at https://www.slideshare.net/Yole_Developpement/mems-sensors-packaging-waferlevelpackaging-technology-and-market-trends-presentation-held-byamandine-pizzagalli-on-semicon-west-2016-in-singapore-presentation-by-yole-dveloppement

[11] BACKHAUS, K., ERICHSON, B., PLINKE, W., WEIBER, R., Multivariate Analysemethoden, 6th Ed., Springer, 1990.

[12] PROSSER, A., WIJAYALATH, L.D., Simulation-based Analysis of Device Availability under three Maintenance Strategies, Transylvanian Review of Administrative Sciences, to be published.

[13] W3C, SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C, 2007, download from https://www.w3.org/TR/soap12/

[14] PROSSER, A., OSSIMITZ, M.-L., Data Warehouse Management Using SAP BW, UTB, 2001.

[15] KLETTI, J. (ed.), MES-Manufacturing Execution System, 2nd Ed., Springer, 2015.

[16] ALMADA-LOBO, F., The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES), in Journal of Innovation Management 3/4 (2015), pp. 16-21.

[17] BOYER, S.A., SCADA: Supervisory Control and Data Acquisition, 4th Ed., International Society of Automation, 2010.

[18] ŠARIĆ, A., MIHALJEVIĆ, B., Smart Parking System in the City of Dubrovnik, download from http://www.rithink.hr/brochure/pdf/vol6_2017/1509301359_4__Andrej___ari____Branko_Mihaljevi___SMART_PARKING_SYSTEM_IN_THE_CITY_OF_DUBROVNIK.pdf

[19] CHOPRA, S., MEINDL, P., Supply Chain Management – Strategie, Planung und Umsetzung, Pearson, 2014.

[20] DUFFUAA, S. O., RAOUF, A., Planning and Control of Maintenance Systems: Modelling and Analysis. 2nd ed., Springer, 1999.

[21] LAND TRAFFIC AUTHORITY SINGAPORE, Intelligent Transport Systems, at https://www.lta.gov.sg/content/ltaweb/en/roads-and-motoring/managing-traffic-and-congestion/intelligent-transport-systems.html

[22] SCHEER, A.W., ARIS – Vom Geschäftsprozess zum Anwendungssystem, 4th ed., Springer, 2002.

[23] PROSSER, A., BAGNATO, D., MÜLLER-TÖRÖK, R., Integration Management with SAP ECC, 3rd Ed., Facultas, 2017.

[24] WASLO, R., LEWIS, T., HAJJ, R., CARTON, R., Industry 4.0 and Cybersecurity - Managing risk in an age of connected production, Deloitte, 2017, download from https://www2.deloitte.com/insights/us/en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html

[25] PROSSER, A., BAGNATO, D., MÜLLER-TÖRÖK, R., The Cryptographic Requirements for Predictive Remote Maintenance Schemes, Transylvanian Review of Administrative Sciences, to be published.

[26] W3C, The Transport Layer Security (TLS) Protocol Version 1.2, W3C, 2008, download from https://tools.ietf.org/html/rfc5246

[27] CCRA, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, 2017, download from https://www.commoncriteriaportal.org/cc/

[28] ROSS, M., IoT-Sicherheitskonferenz: Unsichere Smart-Meter, Mirai und seine Klone und die Genfer Konvention, download from https://www.heise.de/ix/meldung/IoT-Sicherheitskonferenz-Unsichere-Smart-Meter-Mirai-und-seine-Klone-und-die-Genfer-Konvention-3872793.html

[29] THE GUARDIAN, Smart electricity meters can be dangerously insecure, warns expert, download from https://www.theguardian.com/technology/2016/dec/29/smart-electricity-meters-dangerously-insecure-hackers

[30] TURNER, M., BUDGEN D., BRERETON, P., Turning software into a service, Computer 36(10), 2003, pp. 38-44.

Open Data

REVISITING OPEN DATA RESEARCH THROUGH THE LENS OF THE DATA VALUE CHAIN

Csaba Csáki[1] and Andrea Kő[2]

DOI: 10.24989/ocg.v331.17

Abstract

While the idea of open government data is not new, there appears to be a constant shift in leading research objectives guiding the field. This is because the reasons behind the increased research interest keep changing. The latest motivation stems from economic arguments, namely the reuse of public sector information) – which in turn creates a market for open-data based value added services. Although over the last decade many research topics have been identified and various research agendas have been proposed, most of them either focus on specific areas or are rooted in the popular approach of the time. Using the idea of the data value chain, this paper provides an integrated view of open government data research – which then allows a systematic and consistent identification of research topics and clarification of corresponding open questions in the area of open data quality. Research areas proposed are context/environment (policy and regulations), supply side (government organizations), consumer side (service providers and users), (societal or economic) impact, and technology (supporting the DSC, including the data). In addition – and what is regularly missing from most reviews – theory (providing definitions and a sound base) is considered as the sixth area.

1. Introduction

While the idea of open government and making public sector data available is not new [41], the idea keeps returning to the forefront of academic interest. While it is originated in the (typically constitutional) right of access to information and is often requested under the goal of transparency and accountability [22], over the last two decades it has gotten new fuel from the technology backed e-Government initiative [18; 28; 5]. The latest push to access even more public sector information (PSI) comes from commercial interest, namely the trend to apply open government data (OGD) in innovative value added services [10; 26; 55; 54]. "*One of the key purposes of open data platforms is to promote access to government data and encourage development of creative tools and applications to engage and serve the wider community through the visualisation of patterns and relationships*" [52, p. 287]. "*Governments have started to share and open up their own data, yet the real value of open data often comes from integrating government data with non-government data sources*" [46, p 1]. Given the increased interest in open data reuse, the quality of open data has become even more important [49]. There are many research frameworks and models [7] – including open data quality (DQ) measurement approaches [49; 53; 42] – but most of them do not provide avenues to investigate OGD quality in the context of integrated utilization (where data from several sources are combined to create services customers willing to pay for [6]). Furthermore, reuse is not the final goal, instead the real value is in the impact of those utilization efforts [9]. Reuse related open data quality is often addressed under the umbrella of linked open data (LOD), where one of the main concern is provenance of the data sets used [40]. Even though quality is often judged by knowing something's origins and how it was produced, LOD and provenance only addresses some

[1] Corvinus University of Budapest, csaki.csaba@uni-corvinus.hu
[2] Corvinus University of Budapest, andrea.ko@uni-corvinus.hu

of the quality issues, such as difficulties with identifying the origin of data or inability to connect separate datasets [25]. One of the most advanced views of open data is built around the concept of ecosystems [19; 45]. This approach, however, provides a complex analytical model setting focusing on relationships and flows and less readily applicable to the concern of quality. Even specific frameworks dedicated to the issue of quality in the context of open data may only focus on providing dimensions and characteristics of quality or may offer mathematical formulas to provide measurement of quality parameters (upon which OD quality assessment may be based) [49] – but most of them fell short when it comes to offering guidelines what to do about quality lapses identified.

To address the root causes of OD quality issues and to identify when and how quality defects are introduced into datasets (eventually published as open data) a new view is required to allow for new research focus to be established and new research questions to be posed. To this extent this research proposes the application of the 'data value chain' metaphor [20] to establish a research framework within which deeper research questions may be asked in the open data quality area leading to practical considerations for both issuers and users of open data. This paper is organised as follows: after a review of key terms and various frameworks proposed in the open data quality field, the concepts of 'data supply chain' and 'data value chain' are discussed. This is followed by the application of the value chain model to open data – leading to new research topics and questions in relation to OD quality control. The paper is completed by reviewing the key recommendations and proposing further research directions.

2. Value creation and quality in Open Government Data

While the term 'open data' (OD) may cover a lot of different data from differing sources – including scientific and private datasets (Link) – open government data is "*non-privacy-restricted and non-confidential data, which is produced with public money and is made available without any restrictions on its usage and distribution*" ([23], p. 258). Originally, the idea of publishing public sector data (PSD) was the result of promoting accountability and transparency [22]. Later the e-Government idea [18], then the push for open government led to increased demand for Open Government Data (OGD). The latest trend is based on economic interest, namely the idea of innovative, commercial reuse of public sector information (PSI). However, with the advent of commercial reuse [4] – including integration with other, existing datasets (forming mashups) [4] – the focus becomes how value is created and what role quality plays in these processes [10]. While in technical terms data differs from information – the former being a term related to the storage and preservation of symbols (in itself having no meaning), while the latter referring to data interpreted by an actor in a given context [33] –, reusing open data typically means contextual matching, which is thus interpreted as information by the end user. From this point of view there appears to be little differentiation between data and information in the OD literature, especially so when it comes to the question of quality.

It is self-evident that low information quality (IQ) is one of the most difficult and pressing problems for consumers of information, especially given the explosion in the number of informational outlets. But 'quality' can be an elusive concept. There are different frameworks from which information (or data) quality issues can be assessed. For example, adopting a technical view mandates associating information quality with the accuracy of the information in products such as databases. This may be viewed as 'data system quality', looking at issues surrounding timeliness of update, system reliability, system accessibility, system usability and system security [14]. Another, the machine readability approach [13] is concerned with linking, finding, relating and reading data typically

using automated processes [42], and characteristics typically considered include number of formats, traceability, automated tracking, use of standards, trustworthiness, authenticity or provenance. Perhaps the most commonly used simple definition of user side IQ interprets the term as 'fit-for-use' [51]. However, IQ defined this way remains a relative construct whereby data considered appropriate for a given use may not display acceptable attributes in another setting [47]. Furthermore, fit-for-use does not immediately allow for ready measurability and it requires additional detail in order to be operationalized [16]. Moreover, the literature's appreciation of specific characteristics of information quality reveal that the number, definition, and measurability of recommended features or dimensions varies widely. This motivates [44] to state (p. 2): "*Generally speaking, data quality can be related to a set of "dimensions" that are usually defined as quality properties or characteristics*".

Potential IQ criteria may be classified based on whether they are related to the user, to the information itself or to the manipulation of the underlying data [36]. Even though the use and application of quality frameworks expand, they remain focused on the underlying technical and data aspects of IQ. Ultimately, however, it is the user who must decide between qualitatively good and poor information and whether there is an acceptable level of quality required to achieve certain goals and if data is usable to generate value. Indeed, [29] distinguishes accuracy, authority, currency and novelty as quality dimensions. In a similar perspective, [37] differentiated information quality based on accessibility, actual value, completeness, credibility, flexibility, form, meaning over time, relevance, reliability, selectivity and validity. Considering a user-centric perspective of the Internet, information quality would identify the degree to which information is suitable for doing a specific task by a specific user in a certain context [12]. This should hold for OGD as well, yet it is also easy to imagine that given the context, quality expectations for open data might dramatically diverge from data and informational quality issues associated with private data and there may be additional considerations that are special to open data. It is safe to assert that users of open data seek information which may or may not be readily available in the published data set. Indeed, that is the basis for value added services.

One open data quality (ODQ) approach considers technical abilities and concerns raised deviate little from those associated with general DQ investigations. They are concerned about the processes and outcomes of producing and managing datasets as well as about corresponding technical standards [48; 16]. Another stream is centred on the availability and accessibility of various types of data. As an example, the Open Data Barometer [8] raises awareness about the gap between data haves and have-nots on several different availability measures of open datasets around the world. Other related concerns cover whether intended audiences are aware of the availability of relevant datasets and even if they are, whether data is easy to find. Yet another set of frameworks is concerned about specific sectors and take into account the content of the datasets. Finally, it is customary to ask about the value of open data, which, in general terms considers the needs of end users [16]. The current disposition of ODQ characteristics is aptly demonstrated by the work of [53] who, in pursuit of the measurability of ODQ, define and operationalize 68 metrics along 6 dimensions. The Linked Open Data (LOD) 'movement' concentrates on provenance that may enrich the context of open data [40]. Key principles concern the traceability and informational links about the source, the structure of data provenance, linkages to individual elements and linking provenance records. Therefore, dimensions such as origin, attribution, traceability, accessibility and presentation can provide evidence for supporting the assessment of quality, including reliability and trustworthiness. In addition, LOD discussions often centre on potential privacy issues.

However, the core of the literature on IQ/DQ focuses on assessment only. there is a dirt of literature actually providing open data quality control guidelines or even offering best practices. For a data provider organization to be able to provide quality control [49] it would be necessary to know where and why quality issues occur or are introduced. Even quality guidelines fall short of an answer as they only focus on the organizational process and tend to forget about important factors of the public sector setting. Limits of these views with respect to reuse requires a more sophisticated understanding of the relationship between the processes producing OGD and the quality requirements of the various users creating and utilizing value added services. Even though the proposed frameworks and models explaining various aspects of the OGD phenomena regularly refer to "supply" and "demand" most of them do not provide a definition or at least a consistent view of these sides and their related relevant processes potentially introducing errors into the datasets as published and used. Works analysing roles and offering some recommendations tend to focus on after-the-fact quality control by checking datasets prior to release and only for technical issues [49, 21]. This paper considers *the data value chain model* to identify areas of research where insights about quality root causes and corresponding remedies may be uncovered.

3. The concept of a "data value chain"

Viewing data as a result of production-like activities originated in the 1990s. It was [2] who first used the notion of 'information manufacturing'. Then [50] advanced a data quality framework based on the similarities between the two manufacturing processes: in the 'data supply chain' (DSC) "*an information system can be viewed as a data manufacturing system acting on raw data input*" (p. 623). Supply chain is a system of organizations, people, processes, technology, information and resources in moving a product or service from the supplier to the customer (consumer). Data management often discussed as production, storage and application of data in creating value for some end user. Indeed, [50] had already proposed this to be extended into the concept of the 'data value chain' (DVC). "*Use of the term "data product" emphasizes the fact that the data output has value that is transferred to customers, be they internal or external to the organization*" (p. 624). This metaphor bodes well with the idea of OGD reuse, as the final goal is to generate some (societal or economic) value. Later [38] pointed out the importance of a formal 'quality assurance' in the DSC and warned about the importance preventing errors happening.

The data supply chain has resurfaced again when [17] investigated transparency and reliability of linked open data using the DSC. He raised important questions such as who is responsible for an error, or whether the information comes from a curated source. In essence he raised issued of provenance through the supply chain metaphor. Here the supply chain begins when data is created, then it is imported or combined with other data (creating new data), then data moves through the supply chain often being further transformed [32] (and eventually reused). [35] even extended the DVC approach to discuss issues of Big Data. Although the focus is on organizational decision making, they investigate how to bring disparate data together, which is relevant for the mashup-like expectations in OGD reuse. Their model consists of three key data processes with various steps in each: discovery (collect and annotate, prepare, organize), integration (integrate), and exploitation (analyse, visualize, make decisions). Indeed, the Big Data industry relies on constructing data supply chains [32], where exchange and integration of data across different platforms is at the heart of creating value. One issue with the above view of a data (supply and) value chain (summarized in Figure 1) is its 'linear' nature. When discussing the use of raw data, authors often use the 'data lifecycle' metaphor [39] instead, which focuses the attention on the fact that producers of data are also consumers from a different perspective. In summary, while the supply chain and lifecycle approaches focus on 'producers' and 'consumers' (or 'supply' and 'demand'), the value chain

approach considers the context and the processes of transforming components of data into valuable information to be used for some end.

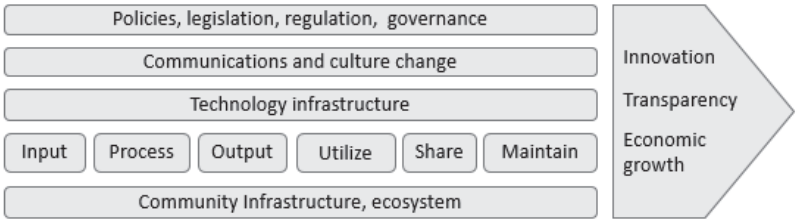

Figure 1: Data Value Chain (based on [20])

As for the supply or producer side, open data is usually (and originally) published in static platforms such as government web portals [43]. Reuse introduces several roles on the 'demand' or consumer side: access providers, cleaners, integrators, service developers and so on, all contributing to increase the value of data and provide benefits – resulting in, hopefully, social and economic impact. While [1] considered the possibility of discussing open data as a value chain, his conference poster presentation has not been explored further. Consequently, this research now turns to the application of the value chain model to the open government data research field.

4. Methodological considerations

To address the issue of preventative data quality guidelines in the context of open data this research applied a systematic literature review followed by theoretical arguments through the application of the data value chain model to the public sector. The research first looked at what relevant research areas had been discussed in the literature, followed by a short investigation considering the special characteristics of the public sector pertaining to opening up their data. Then the data value chain approach is applied to distil research topics with OD quality related questions. For the first part an extensive literature review is utilized [30] searching on specific phrases appearing in either the title, the abstract or the keywords section of papers, namely "open data" and either of the following: "taxonomy", "research areas', "research agenda". Instead of focusing on a basket of journals or a set of leading conferences as is typically done [34], research is based on Google Scholar with the two authors separately sorting out the results leading to 9 papers with meaningful OGD research areas, taxonomies or agendas. Papers that fit the search criteria, but were too narrowly focused on one area (such as innovation only), or covered only specific domains (such as health) were excluded. Based on the research topics such identified, further systematic analysis was executed to see how they relate to the concepts of the data value chain and what meaningful research directions may emerge. The intent was to identify research areas where insights into the root cause of OGD quality issues may be uncovered.

5. Applying the data value chain approach to open government data research

5.1. Open data research: areas and agendas in the literature

Over the last fifteen years or so there appeared regular efforts to review the progress of the field and provide an organization of the various areas within it and propose research agendas. One of the firsts to address the issues of opening up data for reuse was [3], who – while studying these questions on behalf of OECD – proposed 5 domains of a data access regime: technological,

institutional and managerial, financial and budgetary, legal and policy, and cultural and behavioural. While discussing the concept of open government, [19] put forward four domains of OG: policies and practices, users, technology innovation, and context (considering the legal, policy and economic environment), then within this, concluded 6 themes related to open data, namely the workflow of defining data of interest, prioritizing data collection, conducting data collection, publishing the data, using data, and generating value. [9] were interested in the impact of open data and considered 4 'fronts' of scientific interest: history of OD, readiness assessments, implementation studies, and impact studies. [33] focused on research of OD services and their agenda included 7 categories of challenges: Information, Technologies, Processes and Activities, Products and Services, Participants, Customers, and Environment. Reviewing the state-of-the-art of open data related innovation, [55] argue that 7 perspectives should be investigated: legislative, political, social, economical, institutional, operational, and technical - and after reviewing their current state puts forward three research directions: theory and development; policies, use, and innovation; and infrastructures and technologies. [7] has reviewed several research programs (four from those mentioned above) and constructed 35 research topics into four major research areas management and policies, infrastructures, interoperability and usage and value. According to [45] there are 3 points of focus in OGD research: policy and practices, data management, and stakeholder engagement. One of the latest OGD research agendas is [27] with again a focus on innovation and with 3 proposed directions: conducting domain-specific studies, examining the use of tools, and expanding the existing set of research methods and theoretical foundations. [46] constructed an OGD taxonomy from the point of view of cross-sector partnerships consisting of 2 categories (with 6+8 dimensions): data sharing (type, content, admin level, provider diversity, facilitation and access degree of data) and data use (target, selection, policy problems, incentives, continuity, outcome, collaboration, and purpose).

5.2. Special considerations of the public sector in the context of the data value chain approach

There are a few major issues here compared to the traditional data value chain (and lifecycle) models. Data in the public sector has an original role, i.e. it is collected for a specific administrative purpose [31]. Consequently, the way data is collected, stored and manipulated depends on that purpose, which in turn requires transformation to make it reusable – in an unknown context and for goals not related to the original use. Both the original use as well as the process to open up the data is strictly regulated by policies and laws. The producer side thus operates in a strictly regulated context – regarding both data management (collection and storage) and allowing for reuse itself. Freedom of information laws regulated information availability (what must or should not be published, what may be accessible and who can access it); and there are related, but often separate set of rules to govern the issue of reuse (how data such published may be used, what is free and what requires fees to be paid). The producer is strongly separated from the consumer [11]. This is not unlike the inter-organizational information ecology model discussed by [15], where there is a clear split between producers and suppliers when sharing information resulting in disjoint processes. The argument thus can be made that in the context of OGD there are two (asymmetric) data lifecycles: one on the producer side (public entities) and one in the consumer side (commercial re-use of open data in value added services) [11; 39]. This setting is further emphasized by the infomediaries put forward in the ecosystem approach [24], who clean, sort, interpret, reformat, link, and improve the data. Since a "*key quality principle is that customers define quality*" ([21], p. 560), the above specialties result in new challenges of quality going beyond the traditional views of data quality. Consequently, OGD requires improvement both in usability and technical qualities (with the latter including IT-DB qualities of the data as well as provenance and linkages to other data sets). Therefore, to create more value and to improve the quality of the end product (i.e. the services

based on integrated data sets) a close partnership between the supply and demand of data is necessary [46]. To close the loop special feedback channels need to be created [19]. Any research addressing issues in the field of OGD quality should be able to deal with this context.

5.3. Key research areas based on the data value chain approach

Considering the arguments above, the following research areas proposed based on the application of the DVC model to OGD quality: 1) context/environment (policy and regulations – legal background and governance), 2) supply side (government organizations), 3) service providers (on the consumer side), 4) end users and societal or economic impact (also on the consumer side), and 5) enabling technology (supporting the DVC, including the data). In addition – and what is regularly missing from most reviews – theory (providing definitions and a sound base for research) is considered as the sixth area (see Figure 2).

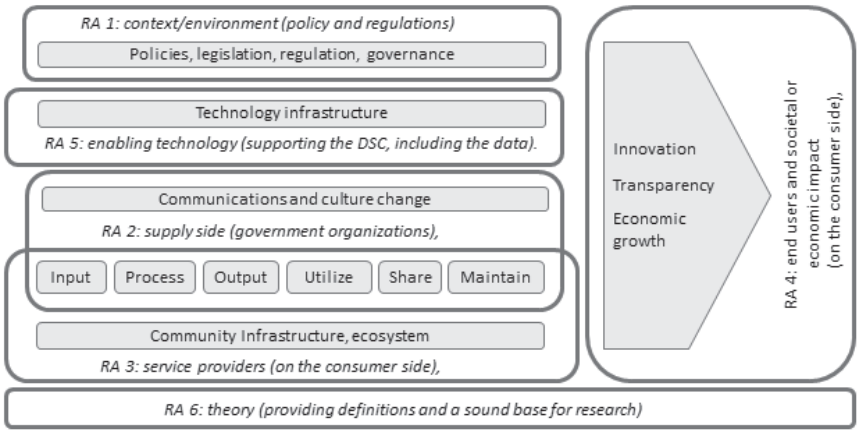

Figure 2: Open Government Data Quality Research Areas (RA) in the Data Value Chain

Context/environment – Legal background and governance: Contextual elements include policy making and legislative actions forming the legal background as well as the processes implementing the resulting regulatory setup. Policy clarifies strategic directions under which regulations should be drawn up and institutions should be organized, while the legal framework creates the context for the rest of the perspective (through publishing and reuse rules), however, a governance element is required for the operationalization of the relevant policy and legal expectations. Research question thus should focus on 1) Are information quality issues considered during the legislative process (what is the level of awareness)? 2) Do resulting regulations reflect quality expectations of end users and if yes, how? 3) How regulatory requirements may introduce restrictions on quality control capabilities?

***Supply side – Governmental organizations*:** Agencies at all levels of governing are involved in implementing OGD policies, or following data publication rules. Research questions of the organizational aspect consider decisions, management processes, and roles: 1) What governance processes may support quality control of OD? 2) What type of errors are associated with the original data management and use process? 3) At which points of the data management process such errors occur? 4) What other errors may be introduced during the generation (publication) of open data?

Consumer side – Service providers: Once open data is 'out there', it is difficult for the originator to control what happens to it. One typical way of dealing with such issues is to restrict the actual use or even charge money – which could defeat the purpose. Therefore, questions of interest here are: 1) What are the quality issues committed by the value added service providers? 2) What quality control mechanisms could re-user install? 3) How to provide feedback: what channels exists to indicate errors or clarify questions?

Consumer side – End users and (societal or economic) impact: According to the re-use model, end users are often even further removed from the 'source'. What is most important here is similar to the service creator role: 1) How to provide feedback: what channels exists to indicate errors, issues or clarify questions?

Technological enablers: Technology plays a crucial role, obviously, in managing the open data value chain. Public entities manage data portals but often provide a platform to engage with their data. There are existing and emerging standards supporting various aspects of the DVC. Data in itself has not been considered as a separate area of interest here, because while data is important, it is not the source of any potential quality issues. Questions: 1) What is the impact of various architecture on information quality? 2) How technology and standards can be used to restrict the likelihood of introducing errors during the data management process (e.g. digitization and various transformations)?

Theoretical foundations: While there are numerous frameworks dealing with OD quality, their main shortcoming is the lack of quality control guidelines. Theoretical treaties of OD quality should provide definitions and a sound base for research – also including critical views as well as historical overviews, reviews of trends and research agendas. Such frameworks should go beyond enumerating quality dimensions and offering measurement addressing research questions related to quality control recommendations: 1) Is there special typology of OGD quality errors and issues? 2) How to overcome the limitations of existing frameworks regarding DQ control? 3) What are the preventative actions offered or discussed in existing case studies? 4) How open data quality maturity models may be used to improve pre-emptive quality control mechanisms?

6. Conclusions and Future Research

Open data quality related research got remarkable interest in the literature. Several papers investigated OD from many aspects, but in the majority of the cases the holistic approach of the discussion is missing, as we detailed in our literature review. We analysed various frameworks proposed in the field of open data quality and highlighted research gaps. Detailed study of these frameworks led us to select data value chain, as a framework for our discussion. The paper has provided an integrated view of OGD research using the data value chain approach – which then has led to a systematic and consistent identification of research topics. We identified six main research areas: 1) environment; 2) government organizations; 3) service providers; 4) end users and impact; 5) technology; and 6) theory. The main advantage of the approach provided here is that it allows for the clarification of open questions corresponding to the given areas – with special focus on the quality of open government data that can be used in value added services. Using the questions posed above, the next step in this research is to focus on the root causes of OGD quality issues and to create a model allowing for the analysis of those causes with the intent to find remedies, such as best practices in quality issue prevention. One model that could also be investigated in relation to the value creation from open data is the ecosystem approach to see if that offers new avenues to insights. The ecosystem model deals with roles and their dynamic relationships in creating value in

ecologies. It would be then possible to investigate the root causes of ODQ issues in relation to those roles and their activities including the nature of communication among them.

7. Acknowledgement

This work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" and of the Corvinus University of Budapest.

8. References

[1] ALBANO, C.S., Open government data: A value chain model proposal, Poster presented at the 14th Annual International Conference on Digital Government Research, Quebec City, Canada, June 17–20, 2013.

[2] ARNOLD, S.E., Information manufacturing: the road to database quality, in: Database 15(5), 32-39, 1992.

[3] ARZBERGER, P., Schroeder, P., Beaulieu, A., Bowker, G., Casey, K., Laaksonen, L., and Wouters, P., An international framework to promote access to data, in: Science, 303(5665), 1777–1778, 2004.

[4] ATTARD, J., Orlandi, F., Scerri, S., Auer, S., A systematic review of open government data initiatives, in: Government Information Quarterly, 32(4), 399-418, 2015.

[5] BERTOT, J.C., Gorham, U., Jaeger, P.T., Sarin, L.C., and Choi, H., Big data, open government and e-government: Issues, policies and recommendations, in: Information Polity, 19(1, 2), 5-16, 2014.

[6] CHAN, C.M., From open data to open innovation strategies: Creating e-services using open government data, in: Procs. of the 46th Hawaii International Conference on System Sciences, 1890-1899, 2013.

[7] CHARALABIDIS, Y., Alexopoulos, C., and Loukis, E., A taxonomy of open government data research areas and topics, in: Journal of Organizational Computing and Electronic Commerce, 26(1-2), 41-63, 2016.

[8] DAVIES, T., Open Data Barometer. 2013 Global Report, online at: http://www.cocoaconnect.org/publication/open-data-barometer-2013-global-report, last downloaded January 21, 2017.

[9] DAVIES, T. and Perini, F., Researching the emerging impacts of open data: revisiting the ODDC conceptual framework, in: The Journal of Community Informatics, 12(2), 2016.

[10] DAWES, S.S. and Helbig, N., Information Strategies for Open Government: Challenges and Prospects for Deriving Public Value from Government Transparency, in: Wimmer, Chappelet, Janssen, and Scholl (Eds) 9th IFIP 8.5 Conference on Electronic Government, Springer LNCS-6228, 50-60, 2010.

[11] DE KEYZER, M., Loutas, N., and Goedertier, S., The Linked Open Government Data & Metadata Lifecycle, https://joinup.ec.europa.eu/sites/default/files/d2.1.2_training_module_2.1_the_linked_open_government_data_lifecycle_v1.00_en.pdf, last accessed November 11, 2017.

[12] EMAMJOME, F.F., Rabaa'i, A.A., Gable, G.G. and Bandara, W., Information quality in social media: a conceptual model, in: Proceedings of the Pacific Asia Conference on Information Systems, Seoul, 2013.

[13] ERICKSON, J.S., Viswanathan, A., Shinavier, J., Shi, Y. and Hendler, J.A., Open Government Data: A Data Analytics Approach, in: IEEE Intelligent Systems, 28(5), 19-23, 2013.

[14] FOX, C., Levitin, A., and Redman, T. C., Data and data quality: Total Data Quality Management Research Program, Sloan School of Management, MIT, Boston, 1995.

[15] FEDOROWICZ, J., Gogan, J.L., and Ray, A.W., The ecology of interorganizational information sharing, in: Journal of International Information Management, 13(2), 1, 2004.

[16] FRANK, M. and Walker, J., User centred methods for measuring the quality of open data, in: The Journal of Community Informatics, 12(2), 47-68, 2016.

[17] GROTH, P., Transparency and reliability in the data supply chain, in: IEEE Internet Comp., 17(2), 69-71, 2013.

[18] GRÖNLUND, Å. and Horan, T. A., Introducing e-gov: history, definitions, and issues, in: Communications of the Association for Information Systems, 15(1), 713-729, 2004.

[19] HARRISON, T. M., Pardo, T. A., and Cook, M., Creating open government ecosystems: A research and development agenda, in: Future Internet, 4(4), 900-928, 2012.

[20] HUGHES, J., An Open Data Value Chain: Making Data Flowers Bloom, London Data Store 31, 2011, online at https://www.slideshare.net/janet-hughes/open-data-value-chain, last downloaded December 15, 2017.

[21] HUH, Y.U., Keller, F.R., Redman, T.C., Watkins, A.R., Data quality, in: Inf. & SW Tech., 32(8), 559–565, 1990.

[22] JANSSEN, K., The influence of the PSI directive on open government data: An overview of recent developments, in: Government Information Quarterly, 28 (4), 446-456, 2011.

[23] JANSSEN, M., Charalabidis, Y. and Zuiderwijk, A., Benefits, adoption barriers and myths of open data and open government, in: Information Systems Management, 29(4), 258-268, 2012.

[24] JANSSEN, M., and Zuiderwijk, A., Infomediary business models for connecting open data providers and users, in: Social Science Computer Review, 32(5), 694-711, 2014.

[25] JETZEK, T., Managing complexity across multiple dimensions of liquid open data: The case of the Danish basic data program, in: Government Information Quarterly, 33(1), 89-104, 2016.

[26] JETZEK, T., Avital, M., and Bjorn-Andersen. N., Data-driven innovation through open government data, in: Journal of theoretical and applied electronic commerce research, 9(2), 100-120, 2014.

[27] KANKANHALLI, A., Zuiderwijk, A., and Tayi, G. K., Open innovation in the public sector: A research agenda, in: Government Information Quarterly, 1(34), 84-89, 2017.

[28] KASSEN, M., Globalization of E-government: Open Government as a Global Agenda, Benefits, Limitations and Ways Forward, in: Information Development, 30(1), 51-58, 2013.

[29] KLOBAS, J.E., Beyond information quality: fitness for purpose and electronic information resource use, in: Journal of Information Science, 21(2), 95-114, 1995.

[30] KRIPPENDORFF, K. H., Content Analysis - An Introduction to Its Methodology, Sage Publications, 2013.

[31] KUK, G., and Davies, T., The roles of agency and artifacts in assembling open data complementarities, in: 32nd Int. Conf. on Inf. Systems, 2011, online at: http://eprints.soton.ac.uk/273064/, last downloaded Dec. 15, 2107.

[32] LI, P., Wu, T.Y., Li, X.M., Constructing data supply chain based on layered PROV, in: The Journal of Supercomputing, 73(4), 1509–1531, 2017.

[33] LINDMAN J., Rossi, M., and Tuunainen, V., Open Data Services: Research Agenda, in: Proceedings of HICSS-46, 1239-1246, 2013.

[34] LINK, G.J.P., Lumbard, K., Conboy, K., Feldman, M., Feller, J., George, J., Germonprez, M., Goggins, S., Jeske, D., Kiely, G., Schuster, K., and Willis, M., Contemporary Issues of Open Data in Information Systems Research: Considerations and Recommendations, Communications of the AIS, Vol. 41 , Article 25, 2016.

[35] MILLER, H.G. and Mork, P., From data to decisions: a value chain for big data, in: IT Profes., 15(1), 57-59, 2013.

[36] NAUMANN, F. and Rolker, C., Assessment methods for information quality criteria. in: Proceedings of the 5th International Conference on Information Quality, Humboldt-Universität zu Berlin, 148-162, 2000.

[37] OLAISEN, J., Information quality factors and the cognitive authority of electronic information, in: Wormell I., Information quality: Definitions and dimensions, Taylor Graham, London, 91-121, 1990.

[38] OLSON, J. E., Data quality: the accuracy dimension, Morgan Kaufmann, 2003.

[39] PARSONS, M.A., Godøy, Ø., LeDrew, E., De Bruin, T.F., Danis, B., Tomlinson, S., and Carlson, D., A conceptual framework for managing very diverse data for complex, interdisciplinary science., in: Journal of Information Science, 37(6), 555-569, 2011.

[40] PIGNOTTI, E., Corsar, D. and Edwards, P., Provenance Principles for Open Data, in: Proceedings of DE2011.

[41] PARKS, W., The open government principle: applying the right to know under the constitution, in: The George Washington Law Review, 26(1), 1-22, 1957.

[42] RULA, A. and Zaveri, A., Methodology for assessment of linked data quality, in: Proceedings of the 1st Workshop on Linked Data Quality at the 10th International Conference on Semantic Systems, 2014.

[43] SÁEZ MARTÍN, A., Rosario, A.H.D., and Pérez, M.D.C.C., An international analysis of the quality of open government data portals, in: Social science computer review, 34(3), 298-311, 2016.

[44] SCANNAPIECO, M. and Catarci, T., Data quality under a computer science perspective, in: Archivi & Computer, 2, 1-15, 2002.

[45] STYRIN, E., Luna-Reyes, L.F., and Harrison, T.M., Open data ecosystems: an international comparison, in: Transforming Government: People, Process and Policy, 11(1), 132-156, 2017.

[46] SUSHA, I., Janssen, M. and Verhulst, S., Data collaboratives as a new frontier of cross-sector partnerships in the age of open data: taxonomy development, in: Proc.s of the 50th Hawaii Int. Conf. on System Sciences. 2017.

[47] TAYI, G.K. and Ballou, D.P., Examining data quality. Communications of the ACM, 41(2), 54-57, 1998.

[48] UBALDI, B., Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives, OECD Working Papers, No. 22, 2013, online at http://dx.doi.org/10.1787/5k46bj4f03s7-en, downloaded Dec. 10, 2017.

[49] VETRO, A., Canova, L., Torchiano, M., Minotas, C.O., Iemma, R., and Morando, F., Open data quality measurement framework: Definition and application to open gov. data, in: Gov. Inf. Quart., 33(2), 325-337, 2016.

[50] WANG, R.Y., Storey, V.C., and Firth, C.P., A framework for analysis of data quality research, in: IEEE transactions on knowledge and data engineering, 7(4), 623-640, 1995.

[51] WANG, R.Y., and Strong, D.M., Beyond accuracy: What data quality means to data consumers, in: Journal of Management Information Systems, 12(4), 5-33, 1996.

[52] WEERAKKODY, V., Irani, Z., Kapoor, K., Sivarajah, U., and Dwivedi, Y.K., Open data and its usability: an empirical view from the Citizen's perspective, in: Information Systems Frontiers, 19 (2), 285-300, 2017.

[53] ZAVERI, A., Rula, A., Maurino, A., Pietrobon, R., Lehmann, J. and Auer, S., Quality assessment methodologies for linked open data, in: Semantic Web Journal, 1(5), 1-31, 2012.

[54] ZELETI, F.A., Ojo, A., and Curry, E., Exploring the economic value of open government data, in: Government Information Quarterly, 33(3), 535-551, 2016.

[55] ZUIDERWIJK, A., Helbig, B., Gil-García, J.R., and Janssen, M., A Review of the State-of-the-Art and an Emerging Research Agenda, in: Journal of Theoretical and Applied Electronic Commerce, 9 (2), 1-8. 2014.

THE NEED FOR STANDARDS – TOOLS FOR TRANSPARENCY AND OPEN DATA (THE CASE OF THE REPUBLIC OF MOLDOVA)

Alexandru Petrov[1] and Cristina Petrov[2]

DOI: 10.24989/ocg.v331.18

Abstract

The Government must make transparency and open data a key priority, as it encourages responsibility, drives development in public services by informing choice, and stimulates innovation and growth. The move to greater openness and transparency is part of a transformation process. Due to nonexistence of transparency standards at the local level, the municipalities' websites differ in terms of structure and published data.

These conditions do not provide sufficient access to data of citizens' interest. Also, there is neither predictability in searching data, nor they can be compared or processed.

Our main objective is identifying and establishing standards for transparency and open data, that will be useful for citizens, as well as accepted and applied by all local government units.

Keywords: *transparency, information systems, open data, web standards*

1. Introduction

What is an open government? Broadly speaking, an open government is a government that allows and encourages the direct participation of citizens to the information it holds and to the decisions taken by administration. The changes in the lifestyle, the continuous modernization of the Internet and new technologies bring back the subject of open governance in a new context, providing answers to some of its dilemmas.

The United States of America is considered to be one of the leading promoters of the open governance. The objectives stated by U.S. include democracy consolidation and increase in the efficiency of the government act, and the three fundamental principles of an open government are as follows [8]:

- transparency of governance, i.e. unlimited access of the citizens to all the information held by public authorities;
- active participation of the civil society in the decision-making process, in this regard it is important the responsibility of the authorities to act promptly;

[1] The Parliament of Republic of Moldova, Stefan cel Mare bd., 105, Chisinau, MD-2073, Republic of Moldova, alexandru.petrov@parlament.md

[2] Information Society Development Institute, 5A Academiei, Chisinau, MD-2028, Republic of Moldova, cristina.petrov@idsi.md

- cooperation between public institutions and citizens, with the aim of implementing measures, including partnerships, and supporting groups of citizens on local level.

The interest for open government is highlighted also by the establishment of an international initiative, named Open Government Partnership (OGP), based on the Open Government Declaration [5], whereby the signatories declare their commitment to respect the four guiding principles for an open government: increasing the availability of information about governmental activities for the citizens; stimulating and supporting civic participation; implementing the highest standards of professional ethics in public administration; increasing access to new technologies for openness and accountability in the governance.

With the development of new technologies, the information held by public administration has turned into large data sets, which has generated the need for new transparency standards - standards that require data to be published in an open format, being reusable. Recent studies have shown that high-value data sets can contribute to innovation and can be the foundation of successful economic initiatives. A few important studies are "Creating Value through Open Data" by Capgemeni Consuling as part of the European Data Portal [10], "Open Data for Economic Growth" by The World Bank [11], and case studies on Open Data's Impact Worldwide, by a team at the GovLab under the leadership of Andrew Young and Stefaan Verhulst [12].

Thus, citizens can track the management of public resources and the data could be re-used to create new opportunities. Open governmental data are those data provided by public authorities, easy and free to access, reusable and redistributed. Open data must offer the possibility of being processed by automatic means and being delivered in an open format. They must be provided under an open license that would accept the free use of the data, without being limited by intellectual property rights, copyright or sui-generis (original) rights with respect to databases, trademarks or commercial secrets.

Open data is an important method for stimulating innovation and economic development, often being associated with the transparency requirements of the activity of public authorities.

The concept of open data has been highlighted lately as a reaction to the need to reconcile the discourse on public interest information with modern society, in particular as a result of the continuous development of the Internet and communications, the progressive use of Big Data and connecting individuals through social networks. Following the above mentioned, it can be said that open data is the most modern framework and international standard for defining transparency, specific to a good governance.

2. About the Public Government Data Portal date.gov.md

On April 29, 2011, through the Government Ordinance No. 43, the Government of the Republic of Moldova [3] has launched the governmental public data portal www.date.gov.md "in order to ensure the transparency of the decision-making process and the participation of citizens in the act of governance as well as the access of citizens and the businesses to public government data."[4] The Electronic Governance Center (EGC) was appointed responsible for coordinating the development and maintenance of the portal.

The Government has required the ministries, central administrative authorities and other public authorities and institutions to identify three data sets of interest for citizens and businesses on a

monthly basis, to be published on the data.gov.md portal and to ensure the regular update of government data with public character according to the frequency of their collection. The Government's provision does not, however, expressly impose sanctions for non-compliance with the provisions in question.

By launching the data.gov.md portal, Moldova joined the global movement "Access to governmental public data", being the 16th country in the world to open a one-stop counter for open data held by government institutions. The EGC has aimed to bring together on a web platform the open public data sets that state institutions publish with or without regularity on their web pages.

On April 15, 2011, EGC has launched a first version of the open data portal date.gov.md, publishing 67 data sets from 5 public institutions [7].

In June 2011 EGC has developed the Open Data Publication Methodology, explaining in details, step by step, how to use the portal and how to fill in the website with new data sets, etc.

According to the EGC, every institution has assigned a person responsible for the open government data, who was trained to update the portal with new open data sets. As per Open Data Publication Methodology, the participation of the government institutions will be assessed based on the volume of data they make available through the date.gov.md portal, related to the total volume of eligible data (publication of which wouldn't compromise the personal character, confidentiality, security or other aspects). The document doesn't clearly state who and how, within state and public authorities, will decide on the total volume of the eligible open data to be published on the date.gov.md.

On December 14, 2011, EGC has launched a new version of the open data platform date.gov.md and then, in February 2014 the version 3.0 was launched, which is used so far. The published data sets are structured according to the institution that opened them. date.gov.md has one search engine based on the keyword and an advanced search engine, by institution, reference period, recommended data set and keyword. Besides, if the users didn't find the data set they were looking for on the portal, then they might suggest a data set. The visitors of the date.gov.md are further encouraged to participate to the portal improvement and the improvement of search engine in particular.

Currently, there are 49 ministries and central administrative authorities presented on the website and on 9 December 2017, 988 data sets were published on the portal.

On April 4, 2012, by Decision no. 195 [2], the Government has approved the Action Plan for an Open Government for 2012-2013 that includes in the Appendix nr.2 the list of governmental public data to be opened in 2012. The ministries and other central administrative authorities were obliged to undertake the required measures for the full execution and within the set deadlines of all the actions described in the plan. The control over the implementation of the action plan was entrusted to the State Chancellery, as well as to the central administrative authorities, with the support of the e-Transformation Coordinators or the officials designated for Open Government Data. In order to implement the Action Plan, the Government has recommended that the National Participation Council (NPC) set up a sectorial working group to monitor its implementation. In May 2012 the thematic group „Open Government / E-Governance" was created within the NPC.

In the list of governmental public data to be opened in 2012 [1] were included 29 sets of data held by ministries and other central administrative authorities. According to the EGC, the list was drawn

up following public discussions and consultations with civil society representatives and subsequently accepted by public ministries and institutions, as confirmed by representatives of civil society [6]. At the initiative of the ministries there were new data sets included in the list. In some cases vague phrases have been used to define sets of data to be opened (e.g. “data in the field of culture” or “data on the current state of transport field”), which gave the public authorities from the beginning enough space for maneuvers.

In April 2012, immediately after the adoption of the Decision no.195, a record number of data sets (130) were published on the portal, and in May - 64 sets. In the following months, on average 20 new data sets were published monthly, with the exception of November, when 70 new data sets were published.

On December 9, 2017, 49 state and public organizations published 988 datasets on the data.gov.md portal. The first five positions in the top of the most opened ministries and central administrative authorities on the date.gov.md portal belong to the Ministry of Health (125 sets of data), the National Bureau of Statistics (121 sets of data), the Ministry of Internal Affairs (106 sets of data), the Ministry of Economy and Infrastructure (63 sets of data), Ministry of Education (57 sets of data). Other institutions published between 47 and 2 sets of data (see the chart 1)

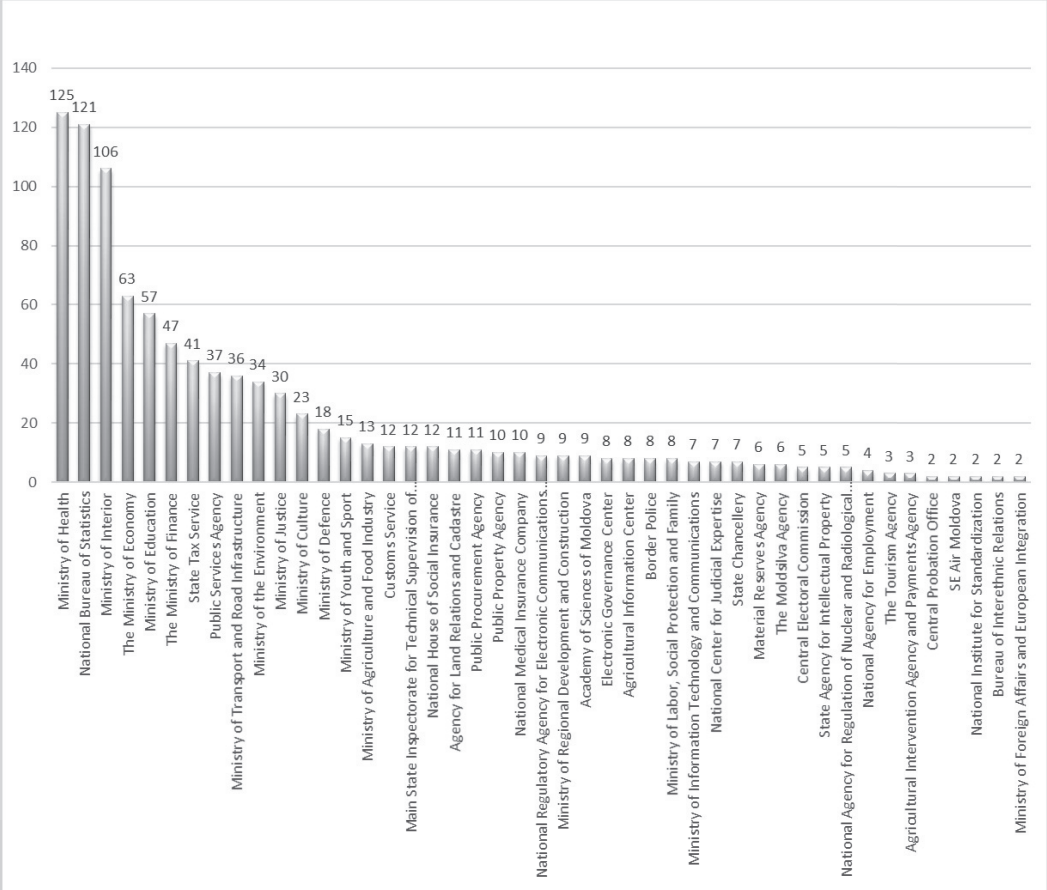

Chart 1: The top of state and public institutions based on the number of datasets published on the date.gov.md portal.

Why do certain ministries and public institutions publish sets of data regularly on the date.gov.md portal, while others don't? Theoretically, the preconditions for a good functioning of the unique office of the open data used by the governmental institutions have been established:

- Every institution appointed a responsible person for the open government data;
- The methodology of publishing these data has been elaborated;
- The appointed responsible people were informed about how to fill out the portal with the datasets.

In reality, a limited number of ministries and central administrative authorities publish datasets on the portal. The reasons of nonparticipation to the process of opening the data available through the portal are:

- The coordinators of open government data are reserved. Once the date.gov.md portal was published they became responsible for publishing the information of public character on the official website of their institutions, as well as on the portal. This assumes a double volume of work, small remuneration, and as a result - zero motivation;
- The lack of clear criteria for defining the complete specter of government data that should be made open by each institution. EGC recommends that the data are selected based on (i) its importance for the citizens, (ii) its importance for the government and (iii) that follows the relevant laws and regulations. The presented criteria allow a range of interpretation to the state institutions, therefore they do not open certain sets of data relevant to the public;
- The bureaucracy in ministries and state institutions complicates the government data coordinator's task of collecting the data from their colleagues from other divisions and subdivisions.

The "The Journey of Open Government & Open Data" study, elaborated by the World Bank in May 2012, identifies several impediments for implementation of the "open data" initiative in Republic of Moldova, that in the authors' opinion, are similar to the ones in countries with democratic traditions, such as Australia, Denmark, Spain, Great Britain and the United States of America. And this includes: an active or passive refusal by the authorities to cooperate in the process of changing the policies in the area of opening the data; marginalization of good practices in data management and data control; juridical barriers and confusion about the legal status of data; the concerns about the wrong data interpretation by the public; feeling of shame for publishing of data of a bad quality; the denial to open the data due to fear of losing an income sources, or due to much secretiveness.

In order to facilitate the access to the data on the portal, it is recommended that the data published by the ministries and the central administrative authorities are to be sorted by:

- the type of published information (i.e. activity report, statistical data, etc.),
- the year of reference (currently users can filter the sets of data by period of reference via the advanced search engine, but not on the subpage of the institution) etc.

Additionally, the governmental institutions should publish the systematized data that they possess for each category of public data for the recent years in an unique format.

On December 26, 2012 the Parliament has adopted the Law no. 305 on re-use of information in public sector (published in "Monitorul Oficial" on March, 29, 2013). The law aims to facilitate the re-use of the documents held by of the public authorities and institutions that have been created during their own public service and could be later used for commercial on non-commercial purposes. The law provides that all authorities and public institutions are required to create lists of documents for re-use via electronic means and in an editable format and to appoint a person responsible for creation of the lists and document directories for re-use, as well as publishing of these documents on the web-page of the authority or the public institution and on the unique governmental portal of open data. As a result, the authorities and public institutions are obligated by the law to open the data of public character to the date.gov.md portal and their own web pages, a fact that could impulse in the near future the process of opening the public information.

3. Recommendations

In order to simplify the access of mass-media, civil society, etc. to the open data sets, published on the official web pages of ministries and authorities of central administration, it is recommended that these would be published on the first page under ¨data of public character¨ or ¨public information¨, or ¨open data¨ rubrics, at one click distance. Additionally the webpage should offer more filter options for published sets of public data, especially by type of activity of the institution, year, etc.

It is recommended to that ministries and public institutions that have online databases or registries of complex data and to publish user guides which include tips and step-by-step instructions for using the database, so-called tutorials or video tutorials. There are good practices in Republic of Moldova in this regard, and is recommended that these are applied by the all the institutions.

In order to ensure the relevance and utility of open data for the mass-media and the civil society, it is recommended:

i) to identify clear criteria to establish the complete specter of governmental data that should be made open by each institution, an exercise that should be carried out by each institution in collaboration with the civil society;

ii) to identify well-defined criteria for publishing the sets of open data, so that these would be complete, comprehensive and actual.

Recommendations for public servants:

i) Corruption likes the secret. There are many cases, in the public sector, as well as in the private sector, when the access to data can contribute to the prevention of corruption. Open data allows more people to be involved in the decision-making process and influence other important activities of public servant.

ii) Opening data improves the efficiency of governments. Public servants may use the data to rely on evidence and as a result react more efficiently to the signals sent by the citizens.

iii) Think openly! Sharing the information with the citizens must be taken into consideration in every case, for all the data.

iv) Do not keep the data to yourselves. Sharing the data improves the efficiency and the will of the public institution, that allow it to develop policies based on evidence.

The open datasets are useless if the public doesn't know about their existence. It is recommended that a governmental strategy for promoting the sets of open data in mass-media, civil society, etc. is developed, and later its implementation through the use of low-cost techniques, as social networks, electronic news blasts, etc.

4. Conclusions

1. An open and democratic society is built on the principle of transparency. Through this principle the civil society exercises its right to know and have access to the information of public interest, as well as over the activity of public authority. As a result of using this right, the civil society can improve the level of transparency of public authorities, improve and develop mechanism for implementation of principle of transparency. The Republic of Moldova has the legal framework necessary to insure a transparent and participating decision-making process, but it is not working efficiently. The national legal framework does not include clear and detailed norms in regard to the mechanisms of control in case of non-transparent decisions. Of course, we must mention that the mechanisms of control and sanctions should not represent a tool of political, financial pressure or of any other kind, on the central public authority, but it should represent an instrument of support, guidance and insurance of respecting the law.

2. The openness has a key role in the service of public sector. Obviously the openness of the public sector should be promoted on all levels. If on a local level we can speak about an implicit openness, due to the proximity of local public administration to the citizen, on the central level mechanisms and special procedures are needed. The existent European experience already identifies re-applicable initiatives in this regard, in the area of governmental openness, as well as in the area of parliamentary openness.

3. The participation of citizens helps the decision-making, improves understanding, cooperation and appreciation of what the public administration does, reduces conflicts, creates the support for application of a project or a plan for community and makes the public administration be more open towards the citizens' problems and concerns. Citizens Participation in a democratic society is fundamental.

The right for information is one of the fundamental human rights, guaranteed by the article 34 of the Constitution of Republic of Moldova. This right cannot be restricted, public authorities being obliged to ensure the correct information of citizens over the public matters and over the problems of personal interest.

5. References

[1] Appendix II to the Government Decision no.195 from April 4, 2012 on the approval of the Action Plan for an Open Government for the years 2012-2013, available at: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=342679

[2] Government Decision no.195 from April 4, 2012 on the approval of the Action Plan for an Open Government for the years 2012-2013, available at: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=342679

[3] Government Ordinance no.43 from 29 April 2011, available at: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=338417

[4] The decision of the Prime Minister of the Republic of Moldova no. 43 of 29 April 2011 with reference to the open administration

[5] The Open Government Partnership - a multilateral initiative that aims to secure concrete commitments from national and subnational governments to promote open government

[6] https://www.opengovpartnership.org/ (accessed on 29.10.2017)

[7] Moldova Open Government Action Plan - process, content and future opportunities, Transparency International, 2012.

[8] The Journey of Open Government & Open Data Moldova, World Bank, 2012

[9] Transparency, Participation, and Collaboration, by Joshua Tauberer, 2014, available

[10] Creating Value through Open Data: Study on the Impact of Re-use of Public Data Resources, by Capgemini Consulting, 2015, available at: https://www.europeandataportal.eu/sites/default/files/edp_creating_value_through_oope_data_0.pdf

[11] Open Data for Economic Growth, by The World Bank, 2014, available at: http://www.worldbank.org/content/dam/Worldbank/document/Open-Data-for-Economic-Growth.pdf

[12] Studies on Open Data's Impact Worldwide, available at: http://odimpact.org/

eGovernment III

THE SHOPPERS; VENUE SHOPPING, ASYLUM SHOPPING: A RESOLUTION IN EURODAC?

Catherine Odorige[1]

DOI: 10.24989/ocg.v331.19

Abstract

The term shopping used in reference to two strictly legal/politically somewhat related issues 'Asylum shopping' and 'Venue shopping', belong to two different spheres of actors. Asylum shopping is descriptive of the action of asylum seekers selectivity, in choice of member state where they perceive better social and welfare conditions. Venue shopping, a concept introduced by Guiraudon in 2000, explain the action of movement by member states in the European Union from venues of national jurisdiction, less amenable to their search for more restrictive migration policy to venues howbeit transnational like transit countries and EU institutions suitable for their policy perspectives. This they did for the primary purpose of avoiding adversary activities of non-state actors and the judicial scrutiny within their national sphere. Common European Asylum System (CEAS) the Dublin Directive and the EURODAC are spill-over in the European integration Project, commonly referred to as the Schengen acquis in the area of migration and integration of third country nationals. The three directives are the results of policy search to administer the entrance and residence of third country nationals especially in the area of irregular migration.

This paper seeks to examine the inter-relationship between the two actors to which the commercial term shopping describes, how an electronic regulation in EURODAC became a check to their 'shopping.' For the asylum seekers exposing their agency, for the member states reducing anxieties, and influenced the ceding of powers hitherto held by member states through (intergovernmental) negotiations to the EU (Supranational) and the impact of these policy measures in checking security challenges and sanitization of this angle of asylum administration in the EU.

1. Introduction

The new political community, which is the result of a borderless EU, a regional system of governance totally at variance with the known systems, dramatically challenged by the establishment of the supranational context in the Treaty of the European Union TEU in 1993 (Wiener 1998 p 4). Since its creation, members of the political community have been in constant search on how to manage challenges that has arisen because of the alliance. Immigration and asylum administration has been on the top agenda because of the removal of security checks at border points where possible external security challenges to the member states are detected. Scholars have attributed the anxiety of member states to the fact that immigration belong to an area of national interest regarded as high politics which relates to the sovereignty of the state (Hoofmann 1965). The 'opt out' and 'opt in' options under the EC treaty agreements reached during the intergovernmental conference of 1996/1997 (Peers 2000; Monar 1998) has enabled countries to choose the extent to which they can participate in certain areas of the Schengen acquis. Both the UK and Irish governments opt out of the Schengen arrangement and still apply border controls at their borders extending to EU citizens. Denmark participate in the Schengen arrangement but opt out of

[1] National University of Public Service Budapest.

the title IV of the EC treaty which makes her participation in the community decisions in the field of asylum and immigration dependent on its classically related to the Schengen acquis.

States asylum and immigration policies have characteristically been restrictive to try to keep out unwanted immigrants from their territory, even in cases of those deserving international protection, which is a provision, made for in the 1951 convention and its 1967 protocol to which member states are signatories. States have overtime avoided the confinement of migration policy to a single national ministry because of its transversal character having implications for range of policy areas like labour economics, foreign and social affairs especially as it relates to admittance and residence of non-citizens (Guiraudon 2000). Criticism on the restrictive policies of member states that undermine the protection of asylum seekers by pro migrants NGO (Freeman 1998; Joppke 1998) is the reasons states in the European Union began to favour cooperation on asylum and migration at the EU level. So called in scholarly literature 'Venue Shopping' which refers to the seeking of new venues by policy makers when encountering difficulties in their traditional policy venue, obstacles to developing stricter migration policies led to the EU level cooperation (Guiraudon 2000, 2003). Member states found a safe haven at the EU level to circumvent domestic obstacles to achieving policy choices on migration (Maurer & Parkes 2007 Lavenex 2006). The venues keep shifting depending on what best suits the interest of the policy makers intergovernmentalist approach or supranational as well as the use of transit countries to manage their migration challenge. The development of the European Union asylum and migration policy, despite the fact that these are related but different policy issues, the main aim is to find ways to keep immigrants out of the EU. (Boswell, 2003, 2007, 2008; Ellermann, 2008; Geddes, 2000; Guild 2004; Lavenex, 1998, 1999, 2001a, 2006; Levy 2005 Thielemann, 2001a, 2006). The cooperation in such field of asylum led to the Common European and Asylum System, which experienced a storm in the wake of the migration, flows in the in 2015. The CEAS determine which country has responsibility for asylum claim through the Dublin regulation, safe country concept, determining asylum claims is a complex procedure where in variety of legal procedures, implemented in individual member states. Regardless of CEAS, there is no uniformity in sight in the way member states determines who get recognition and who does not, or why there are not uniformed percentages in asylum recognition rates across member's states. An example is the report on asylum rates in the 2015/16 of asylum seekers from Syria Germany was 97.4/57.2 percentage while Hungary was 5.7/0.5 % (Burmann & Valeyatheepillay 2017). The differences in interpretation and policy, is determined by what the state perceives as convenient to for its local immigration and integration policy. Despite these various interpretations and implementations along common policy agendas, one area where there has been unanimity is the EURODAC where states, which have chosen to stay out of the Schengen acquis Britain /Ireland, and Denmark who opted out of CEAS as well as the Nordic countries, have been participating in EURODAC.

2. Asylum and Asylum Shopping

Asylum refers to the process by which a person who has lost protection of his state moves to another country to seek for protection. An offshoot of the Universal Declaration of human rights in 1948, the United Nations Convention relating to the granting of refugee status adopted in 1951, which gives recognition to the right of persons to seek asylum from persecution. This convention has been subjected to amendment only by the 1967 protocol, which removed the geographical limits of the 1951 convention (UNHCR). Asylum shopping, a negative connotation refers to asylum seekers perceived agency in choice of destination (Moore 2013). The application for asylum in more than one member state in the EU or chooses a member state over others because of perceived higher standard of reception conditions or social security assistance. (DG Home). The implication

of this agency to policymaking is that it tends to undermine the European integration project to the extent of resulting in regulatory policy to check it. Despite the relevance of this discourse, to the asylum theorizing and administration not much is reflected in academic literature, as much is yet to be done to subject the rhetoric behind the discourse and the social political implication to academic perusal. Though widely acknowledged in the works of (Menz 2009; Muller 2004; Thomas 2003; Wilson 2006). (Moore 2013) represents the emergent academic research on the discourse, centred on the social-cultural meaning of asylum shopping, and how it is naturalised in the British media, so that in 2000 news on asylum and refugee issue were the dominated issues in the media. Asylum seekers were in the news represented as cheating the system, exploiting social resource and scrounging welfare state benefits and social housing. With the politicians and the press implying, that economic migration or more sinister claims were driving the migration (Moore 2013). Regular and irregular movements as possible ways to classify asylum /refugee movements (Jaeger 1988), classifies as 'irregular' movements by *bona fide* asylum seekers because the trip is made under duress. 'Irregular movements' he classifies as movement taken by asylum seekers and refugees after fleeing the country where persecution is feared and the patterns of these movements may not comply accurately to the international community expectations (Jaeger 1988 pp 23-4). Of relevance to this discourse is the description of movements where asylum seekers move from one or more countries because the asylum seeker received neither protection nor asylum, to which Jaeger does not, considered as irregular. Irregular movement he avers as spontaneous, unauthorised, unscheduled arrival of protected asylum seeker or refugees. That is asylum seekers have received some form of protection in one country yet moves in an unauthorised or unscheduled way to another country. Pointing to difficulty in applying the concept of irregular movement due to the challenges of increasing problem of personal documentation, lack of solution to the problem of 'refugee in orbit' the divergent views between jurists, courts and states on such basic topics as 'asylum' and 'protection' (p 25). However, (Moore 2013) explains Jaeger mention of refugee in orbit in terms of his meaning asylum shopping but the refugee in orbit described by Jaeger, moved through the first country as a transit point without applying for asylum there. Which could be for a variety of reasons, ranging from fear of not receiving the refugee status, to possible better reception and welfare elsewhere other that country that is a closer neighbour to the country of his persecution. This has also brought about the controversial country of first asylum, the concept used to establish that some asylum determinations are someone else's business, i.e the countries that first harboured the claimant (Vierdag 1988). The hostilities toward the *others* mostly from post-colonial/imperial nations in Europe (Guilroy 2004, 2005) where the violent histories of post-colonial countries are hidden in hostilities towards those classified as racial other which include immigrants and asylum seekers who are unwanted because they are bearers of imperial and colonial past which these countries are bent or denying.

3. Venue Shopping

Several theories furthered to explain member states move form exclusivity control of migration and asylum in the early stages of the European integration project, a policy area tied to security and sovereignty, which states preferred to keep within their reach away from the jurisdiction of the supranational EU. Difficulty arising from spill over effects of the European integration project, explains this kind of selective policies by two schools of thought, the first stems from theories of international relations that due to globalization states seek international solutions to domestic problems (Keohane & Nye 1989). Decreasing ability of the state to control immigration because of its self-preserving nature, the constraining impact of economic imperatives and international legal norms, and this view, linked to the neo-functionalist view that spillover and consequences from other EU pioneering policies provide the rationale for further common EU policies. The second is

on the state centric intergovernmental view on immigration control, that growing international immigration and crime causes convergance for national preferences as a pre-condition for cooperation. Here the EU provide the framework for member states to cooperate to reducing external negatives and cost of transaction (Moravcsik 1993 and Hix & Hoyland 2011). Spillover is broken down into functional spill-over, political spill-over and cultivated spill-over (Tranholm Mikkelson 1991). In addition, the point made in (Bierman et al 2009) contextual point of conventional wisdom which suggest that spillovers foster issue linkages and further integration. While acknowledging some of these theories Giraudon 2000 citing (Baumgartner & Jones 1993) reference to policy venues analyses the internationalization of migration and asylum control policy as venue shopping. The institutional locations where policies reached through the mobilization of different constituencies, as political actors tend to seek policy venues that are suit their policy choices. Venue shopping emphasizes actor's strategies and the rule bound environment to which actors respond. Seeking new venues in order to adapt to institutional constraint framing processes to policy images the constructivist's moment (Guiraudon 2000). The reasons for the transcendence in policy avenues is first because they are relieved from the judicial constraint from national level, opposition from ministries, parliaments and migrants aid groups are miffed, finally the job of policing have been seconded to transit and sending countries as 'Sheriff deputies' (Torpey 1998).

The rise in asylum seekers in Europe in the 1990s led to the securitization of the issues of asylum (Bigo 1996). Asylum challenges like Asylum shopping and security migration policies experience new venues of its development through coordination via liberal intergovernmentalist approaches of supranational.

Venue shopping that bought the member states to seek international solutions to national challenges to policy implementation was also a relief for the EU, as it needed to foster partnering relationships with the member states especially in contentions issues like migration and asylum. That were major themes in political rhetoric discrediting the European integration project and political actors and the media were fuelling most of the disaffections (Moore 2013). Unfolding reaction to immigration and asylum is evident that countries that pushed for the single market framework in the European integration did not for see the spill over effects that will follow. Among which are the UK and Ireland opted out of EU migration discussions an obvious undermining of the inter-linkages between the two (Guiraudon 2000). The Europe a la carte in the Amsterdam treaty gave room for these opting out of the Schengen acquis and Denmark despite being a member of the Schengen cooperates only in the common visa policy and not the asylum policy. Iceland and Norway membership of the Nordic Passport Union are bound by the Schengen protocol, of the Amsterdam treaty. Neo functionalist theories explains the commission back seat role in the policy drafts acting only in maximizing outlook and agenda setting function (Pollack 1994), considered it wisdom to leave decisions in the these fields to the discretion of the member states in view of the stalemate hitherto experiences in these fields. Therefore, the searches for securitised administration of asylum were realised by the member states.

3.1. Rationale behind EURODAC

EURODAC. An acronym for European dactylographic system, an automated biometric identification allowing for instant and exact comparison of unique physiological features for individual's iris, face and finger print for law enforcement purposes (Aus 2006). The Refugee influx in Europe has put pressure on the member states and these developed and industrialised states look for varying means to constrain the influx, as a check against asylum abuse and 'asylum shopping' in an integrating Europe striving for a full-fledged harmonization of substantive and

procedural refugee law (Aus, 2006). The EU started to develop a Common European Asylum System to improve the framework of the Convention relating to the status of refugees. Several common directives, established in alignment to member states legislation, procedural directive, reception condition directives, and qualification directives. Spill over effect of administering directives led to the development of the Dublin Regulation, which helped establish the state responsible for examining the asylum application, because controversies of country of first asylum and irregular movements (Vierdag 1988; Jaeger 1988) which can be antithetical to an asylum claim regardless of the merits of the case. In addition, the advantage of saving member States involved in the Common European Asylum directive, from conducting "one-to many checks" in this category, is the justification for involvement in the adoption of EURODAC by the Council of the European Union on 12/11/2000 and 02/28/2002 (Council 2000a; 2002). The two dates in the adoption of the Eurodac system is supportive of the argument by (Aus 2003) that securitization of the asylum and immigration policies in the European Union, was not the result of an 'external shock' of the September 11 2001 attack. However, internal institutional dynamics resulting in an imbalance between the principles of freedom security and justice are linked to the first. The first Eurodac directive was passed in 2000 prior to the 9/11 attack, only the second one which came later in 2002 extended to irregular border crossing, illegal residence and EU citizens, after the attack could be linked influences of the attack, providing additional window of opportunity supranational executions of powers. The biometric feature of Eurodac, which allows for immediate identification of unique physiological features, helps member state to determine if an asylum seeker has applied for asylum elsewhere in the European Union. Which is a check against the rate of asylum shopping; the knowledge that they are subject to detection has put a check on asylum seekers agency. The system has also been a security check for detecting terror attacks and criminal acts by individuals pretending to be asylum seekers.

3.2. JHA; Justice and Home Affairs, Area of freedom Security and Justice

The parallelism of the JHA department responsible for freedom security and justice, which takes responsibility for the protection of universal human rights and the right to privacy, being the initiator of the Eurodac regulations; which run contrary to the formal foundations of the department. The extension of the Eurodac database to irregular border-crossing, illegal residence of third country national and EU citizens this is illustrative of the fact that task expansion on European level and executive "fusion" may take place in practice (Aus 2003). Eurodac Regulation is framed as a Dublin-related measure in the field of asylum, passed on the legal basis of art. 63 (1) (a) of the EC Treaty in its currently valid "Nice" version (Ibid). This treaty provision authorizes the Justice and Home Affairs (JHA) Council to adopt Community legislation laying down "criteria and mechanisms for determining which Member State is responsible for considering an application for asylum" lodged in the European Union by a third country national, actors calculating strategy produces political outcomes adherent to the rationalist's logic of consequentiality, which may include supranational legislative acts as the EURODAC. In rationalist analytic framework, purposive-rational actors tend to perform means-end and end-ends calculations culminating in utility-maximizing choices (Aus 2003). Rationality is determined by action taken when the ends, means and secondary results are weighed and accounted for. This involves the rational consideration of alternative means to an end, of relationships to an end of secondary consequences and the importance of different possible ends (Elster 2000, cited in Aus 2003). The rationality in choices made by countries in Europe by the provision given in the a la carte to stay out of Common European Asylum system -Dublin, the Schengen acquis UK and Ireland. However, deciding to cooperate in the supranational structure of the EU in the EURODAC regulation attests to the merits ease of the regulation in the administration of third country national's entre, stay and securitisation

of the target group for ease of policing and asylum administration. (Geddes 2005) however points to the their opt in decision as being at variance with the justification for EURODAC which is tied to the article 61 EC the elimination of border checks to which these countries opted out of. It is allegedly addressing challenges of irregular or secondary movements where it was simply impossible to identify persons, especially asylum shoppers bent on hiding their real identity (Aus 2003).

4. Conclusion

Rational choices of actors' action as it relates to end-means determine actor's decisions. EURODAC electronic features have impacted in no small measure in checking asylum shopping and the security implications of admitting third country nationals in view of the terror anxieties sweeping across the globe. Its advantages for asylum administration are evident in the general acceptance across member's states. Countries like United Kingdom and Ireland who had opted out of the Schengen acquis and Denmark which cooperate in the common visa policy and opt out of the CEAS regardless of being in the Schengen system have all opted in to the EURODAC as a means of checking asylum shopping and also because of the securitarian privilege it offers in the monitoring of third country nationals.

Sociological institutionalists' perspectives challenge the logic of appropriateness, (Olsen 2007) as a common good solution to pressing challenges applied by institutional actors. A closer observation reveals that this logic accounts for political attitudes and behavioural traits of institutional members pursuing other agendas (Arendt 1994). Meaning as appropriate as a logic of action might seem it may be a colour-blind device in the hand of political actors (Aus 2006). However the efficiency of its performance in the area of asylum applications is clear from the number of detections of asylum shoppers across EU member states. The Central Unit detected "asylum shoppers" -persons who lodged applications in more than one member state, 3100 persons between January 2003 to December 2004, these detections were mostly in countries like Germany, Sweden, France, the UK, and Austria (Aus 2003). On the other hand Eurodac have been less successful in illegal border crossing because of the delay by member states in the hotspots of irregular crossings to send information to the central processing unit in a suspicious attempt at undermining the Dublin II directive (Papadimitriou and Papageorgiou 2005). And discovery of second application asylum seekers attempts at defacing their fingers through cutting, burning so as not to be detected through their finger prints of having applied elsewhere for asylum. Finally the 'opt in' decision by hitherto opting out parties like the UK, Ireland and Nordic countries Iceland and Norway to participate in the Eurodac is because of the perception of the relative ease it brings in the face of the security and undermining challenges faced by EU member states in the asylum administration.

5. Bibliography

[1] ARENDT, H., Eichmann in Jerusalem. A Report on the Banality of Evil. Penguin. London 1994.

[2] AUS, J. P., Supranational Governance in an "Area of Freedom, Security and Justice", Eurodac and the Politics of Biometric Control, University of Sussex: Sussex European Institute, Working Paper No. 72. Sussex 2003

[3] AUS, J. P., EURODAC; A Solution Looking for a Problem? European International Online Paper, Vol 10 pp1-26. 2006

[4] BAUMGARTNER, F., & JONES, B., Agendas and Instability in American Politics, Chicago University Press. Chicago, 1993

[5] BIERMANN, F., PATTBERG, P., ASSELT, H., ZELLI, F., The Fragmentation of Global Governance Architecture: A Framework for Analysis. Global Environmental Politics 9, Massachusetts Institute of Technology. 2009.

[6] BIGO, D.,"Frontiers and Security in the European Union: The Illusion of Migration Control," In, Anderson, M. & Bort, E., (eds.), The Frontiers of Europe, London: Pinter, pp. 148-164 1998.

[7] BOSWELL, C., 'The 'external dimension' of EU immigration and asylum policy', *International Affairs,* 79(3): 619-638 2003

[8] BOSWELL, C., Migration Control in Europe after 9/11: Explaining the absence of securitization', *Journal of Common Market Studies,* Vol.45, no.3, pp.589-610. 2007

[9] BOSWELL, C., Evasion, Reinterpretation and Decoupling: European Commission Responses to the 'External Dimension' of Immigration and Asylum', West European Politics, vol. 31, no. 3, pp. 491-512. 2008

[10] BURMAN, M., VALEYATHEEPILLAY, M., Asylum Recognition Rates in Top 5 EU countries https://www.cesifo-group.de/DocDL/dice-report-2017-2-burmann-valeyatheepillay-june.pdf 2017

[11] Council of the European Union "Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention," in: Official Journal of the European Communities of December 15, 2000, Vol. L 316, pp. 1-10.

[12] ELSTER, J., Rationality, Economy, and Society," in: Turner, S. (ed.), The Cambridge Companion to Weber, Cambridge University Press, pp. 21-41. 2000

[13] FREEMAN, G., The decline of sovereignty? Politics and immigration restriction in liberal states', in C. Joppke (ed.), Challenge to the Nation State: Immigration in Western Europe and the United States. Oxford University Press. pp. 86-108. Oxford 1998

[14] GEDDES, A. "Getting the Best of Both Worlds? Britain, the EU and Migration Policy," Oxford. International Affairs, Vol. 81, No. 4, pp. 723-740. 2005

[15] GEDDES, A., 'Lobbying for migrant inclusion in the European Union: new opportunities for transnational advocacy?' Journal of European Public Policy 7(4): 632–49. 2000b

[16] GUILD, E., Seeking asylum: stormy clouds between international commitments and EU legislative measures´, European Law Review, vol.29 (2) April 2004.

[17] GUIRAUDON, V. "European Integration and Migration Policy: Vertical Policy-making as Venue Shopping," in: Journal of Common Market Studies, Vol. 38, (2) pp. 251-271. 2000

[18] GUIRAUDON, V. "The Constitution of a European Immigration Policy Domain: A Political Sociology Approach," in: Journal of European Public Policy, Vol. 10, No. 2, pp. 263-282. 2003

[19] HIX, S., & HOYLAND, B., The Political System of the European Union, third edition, Palgrave Macmillan. London. 2011.

[20] HOFFMANN, S., The State of War; Essays on the Theory and Practice of International Politics. Praeger Publishers. 1965.

[21] JAEGER, G., Irregular movements: the concept and possible solutions. In: Martin D (ed.) The New Asylum-seekers: Refugee Law in the 1980s. The Ninth Sokol Colloquium on International Law. Dordrecht, pp 23-48 Martinus Nijhoff . Netherlands 1988.

[22] JOPPKE, C., (ed)`Challenge to the Nation-State: Immigration in Western Europe and the United States´ Oxford University Press. Oxford. 1998.

[23] KEOHANE, R. O., NYE, J. S., Power and Interdependence. Second edition HarperCollins, London 1989.

[24] LAVANEX, S., The Europeanisation of Refugee Policies. Between Human Rights and Internal Security, Ashgate , Aldershot 2001.

[25] LEVY, C. (2005), 'The European Union after 9/11: the Demise of a Liberal Democratic Asylum Regime? Government and Opposition, pp. 26-59

[26] MAURER, A., & PARKES, R., 'The prospects for policy-change in EU asylum policy: venue and image at the European level', European Journal of Migration and Law 9: 173-205 2007

[27] MENZ, G., The Neolibralized State and Migration Control: The Rise of Private Actors in the Enforcement and Design of Migration Policy. Debatte; Journal of Contemporary Central and Eastern Europe Vol. 17, 315-332, 2009.

[28] MOORE, K., Asylum Shopping in the Neo-Liberal social imaginary DOI: 101177/0163443712372090. SAGE. 2013

[29] MONAR, J., "Justice and Home Affairs in the Treaty of Amsterdam: Reform at the Price of Fragmentation," in: European Law Review, Vol. 23, No. 4, pp. 320-335 1998

[30] MORAVCSIK, A., Preferences and Power in the European Community: A liberal Intergovernmentalist Approach. Blackwell Limited. Oxford. 1993.

[31] MULLER, B., Globalization, security, paradox: towards a refugee biopolitics. Refuge Canada's Journal on refugees' vol. 22, Issue 1, 49–57. 2004

[32] OLSEN, P. O., Understanding Institutions and Logic of Appropriateness: Introductory Essay. ARENA Centre for European Studies, University of Oslo, 2007

[33] PAPADIMIITIOU, P. N., & PAPAGEORGIOU, I. F., "The New 'Dubliners': Implementation of European [sic!] Council Regulation 343/2003 (Dublin-II) by the Greek Authorities," in*:* Journal of Refugee Studies, Vol. 18, No. 3, pp. 299-318. 2005

[34] PEERS, S., Justice and Home Affairs: Decision-making After Amsterdam," in: European Law Review, Vol. 25, No. 2, pp. 183-191. 2000

[35] THOMSON, M., Images of Sangatte; Political Representations of Asylum-seeking in France and the UK. Sussex Migration Working Paper No. 18. Brighton: Sussex Centre for Migration Research, Sussex 2003

[36] THIELEMANN, E., 'The Soft Europeanisation of Migration Policy: European Integration and Domestic Policy Change', Paper prepared for the ECSA 7th Biennial International Conference, May 31 – June 02, 2001, Madison, Wisconsin 2001.

[37] THIELEMANN, E., the Effectiveness of Asylum Policy in Controlling Unwanted Migration, in Parsons C., & Smeeding, T., (eds.) Immigration and the Transformation of Europe, pp. 442-72, Cambridge University Press, Cambridge 2006

[38] TORPEY, J., Coming and Going: On the State Monopolization of the Legitimate Means of Movement. American Sociology Association. DOI 10.1111/0735-2751.00055, vol 16, issue 3, Nov. 1998.

[39] TRANHOLM-MIKKELSON, J., Neo-functionalism: Obstinate or Obsolete? A Reappraisal in the Light of the New Dynamism of the EC. Millennium Journal of International Studies. Vol. 20 No pp 1-22. 1991

[40] UNHCR, Convention and Protocol Relating to the Status of Refugee http://www.unhcr.org/3b66c2aa10.pdf

[41] VIERDAG, E. W., The Country of First Asylum: Some European Aspects; In: Martin D (ed.) The New Asylum-seekers: Refugee Law in the 1980s. The Ninth Sokol Colloquium on International Law. Dordrecht, pp 73-84 The Netherlands. Martinus Nijhoff.

[42] WIlSON, D., Biometrics, borders and the ideal suspect. In: Pickering S, Weber L and Wilson D (eds) Borders, Mobility and Technologies of Control. *Springer,* pp. 87–109, Netherlands 2006.

[43] WIENER, A., European Citizenship Practice; Building Institutions of a Non-State. Westview Press, Oxford 1998.

HOW TO STOP DIGITALIZATION – AN E-GOVERNMENT PILOT PROJECT CASE STUDY

Birgit Schenk and Tobias Giesbrecht[1]

DOI: 10.24989/ocg.v331.20

Abstract
Pilot projects are a means of learning whether the promises of an E-Government-innovation hold true. We analyze the case of an unsuccessful E-Government pilot projects for patterns of obstructive behaviour and their justifications. The identified patterns can serve as early warning signs for endangered pilot projects. Furthermore we use them to deduce recommendations for improving the innovation-readiness of public administrations.

Keywords: *e-government, innovation project, early warning signs, pilot projects, public administration*

1. Introduction

Innovation and change are fundamental to mastering the challenges such as demographic development and the need to be competitive [8]. This is a matter of fact for all organizations in business and public administration at all levels (federal to local) [23].Multilevel reforms and modernization initiatives (e.g. New Public Management) following comprehensive plans under new regulations have taken place or are still being initiated, but the extent of the changes and of the innovation doesn't on the whole meet expectations [16]. Persisting in keeping the status quo seems to be perceived as success within public administration even if it is obvious that competition and sustainability demand change and innovation. Most of the recent innovations are run under the heading of E-Government. Genuine innovations are risky and therefore the public administrative organization tries them out in pilot systems before rolling them out. While there is ample evidence of failed E-Government projects and reasons why they failed [13], there is a lack of studies on how to manage those sensitive pilot systems. As they are set up to explore the operational and organizational feasibility of an E-Government innovation [14], they rely much more on the constructive collaboration of all stakeholders. Thus, monitoring the behaviour of them can be the key to understanding where a pilot-project stands and what should be done. As always, most can be learned from failures. Therefore, in this paper we will analyze a failed E-Government pilot system and ask ourselves: How did the actors manage to stop the project? Or more specifically: Which patterns of obstructive behaviour can be identified and how far are they justified. Those patterns can then be used by practitioners as early warning signs for project failure in future pilot systems and open up the field for specific research on early warning signs for E-Government failure.

[1] University of Applied Sciences – HVF Ludwigsburg, Germany, schenk@hs-ludwigsburg.de, University of Zurich, Department of Informatics, Zurich, Switzerland, giesbrecht@ifi.uzh.ch

2. Background

2.1. Culture of Innovation and Innovation Projects in the public Sector

Innovation is an act of creative destruction [21]. Thus it touches fundamental principles of public administration such as stability, security and the control of public interests [1]. These principles demand employees who are able and willing to cope with stable and inflexible structures, routine, regularity, with comparatively little change in their day-to-day working life and are therefore comfortable with regulations, avoidance of any uncertainty, high power distance etc. At the same time these principles encourage only compatible norms and a compliant organizational culture. Deal and Kennedy call this a process culture [2]. Employees of a process culture concentrate on how to do things correctly because they assume and fear that they will be attacked if they have done things incorrectly. It is a culture of no mistakes, major avoidance of uncertainty, distrust, subordination or conformity. This is the opposite to aspects such as curiosity, trial and error, responsibility, accountability or activities for continuous improvement, etc. that are significant and essential for a culture of innovation. A culture of innovation asks for open mindedness about how to do things and the adaptation of goals, the exchange of project members in accordance with the project phases and tasks, and for employees who are willing to stand out. Taking these facts into consideration it is obvious that there is a cultural clash: the culture of innovation clashes with the culture of public administration. Therefore it is natural for public administration to oppose any innovation.

There are two categories of opponents: the constructive and the destructive [6]. Constructive opponents realize that the innovation cannot be stopped and therefore they try to change the outcome. These changes can be positive, if the constructive opponent is integrated in the process of change and if his knowledge is used to improve the introduction and implementation of the innovation. Destructive opponents try to delay and slow down this innovation or to stop it completely. They disguise their opinions and actions. Their arguments vary all the time according to the circumstances and the situation.

Public officials can be seen as being averse to risks [9]. In the context of change the attitude behind this follows a simple structure. Public officials ask themselves: Are fundamental risks to be expected if I don't change my attitude? If not, they don't do anything anymore. If they answer the question with "YES", then the next question arises: Are there consequences to be expected if I change my attitude? If he doesn't think so, he tries not to cause conflicts and starts to seek and to assess information as well as planning his next steps based on this to avoid change. Pretending to act hides his attitude. If he expects consequences, he asks the next question: Is there any realistic hope of a better solution than the innovation being targeted? If he doesn't see one any better his actions go against the innovation to avoid or slow down its implementation. This is called defensive avoidance. If there is realistic hope he estimates the time he needs to obtain and to assess more information. If there is no time left, he panics and tries to make others responsible and accountable for the problems caused and he stops working on it. [10] What does this kind of behaviour mean for public administration?

Public administration is bound to keep to the principles of equal treatment (non-discrimination) and legal certainty. Valid laws and provisions, regulations and guidelines as well as the resulting tasks are deduced from these principles and result in a special organizational structure with fixed organizational processes. They are tailored to cope with daily work but not tailored to meet the requirements of innovation processes nor introductions nor implementation. Each employee knows his competences and responsibilities according to his hierarchical position and he is strictly bound

to them even if he works on a project. Hierarchical and functional barriers are adhered to [24] and intensified according to Hormon's Accountability Paradox. This says that public officials are obliged to act in compliance with laws, edicts, and rules even if their attitude or opinion is different. According to Hormon the concept of responsibility is central to our ability to deal with contradictory motives and forces. Responsibility has more than one meaning: responsibility describes people as authors and personally responsible for their actions; accountability means that people are answerable to the higher authority for their actions; obligations are moral actions determined by external sources which set standards and principles. These generate conflicts e.g. public officials have to act according to their obligations and against their own attitudes and opinions. So they learn to ignore their own moral principles and are simply executors without personal accountability. Four pathologies are generated:

Passing the buck: They deny personal authorship or having sufficient authority and they deny resources to achieve the institution's goal.

Scapegoating: A person is blamed in order to protect an institution's complicity and its' members illusion of their collective innocence.

Atrophy and Individual Moral Agency: The officials pretend to be the victim and thus discourage the exercise of personal authorship and responsibility.

Avoidance of Individual Responsibility: The relaxation of standards to foster the illusion of the victims' innocence and to foster the lack of confrontation and candour necessary for instilling a sense of personal answerability.

2.2. Early Warning signs for project failure in pilot projects

An early warning sign (EWS) provides an indication of risks arising and pointing to related barriers, difficulties, and/or failures [11]. An EWS typically refers to perceivable symptoms rather than to (invisible) underlying causes [23]. For example, if an important stakeholder frequently excuses him/herself from meeting, this is a visible sign; the underlying cause may range from a conflict of interests to simply a lack of time. Symptoms can relate to (1) client or stakeholder, (2) project's goal, (3) meetings, (4) the team, (5) the task, (6) the project, (7) the project management, (8) communication, (9) the overall management, (10) the project portfolio, and (11) to the process [7].

As EWS are visible they provide an experienced manager with a tool to monitor activities and react early. Pilot projects by definition have a limited scope: their purpose is to test the operational feasibility [6] and thus uncover the precedents and effects of an innovation. Thus top management typically shows a "wait-and-see" attitude. This is in sharp contrast to the established project management knowledge that top management support is key to project success [27]. The less support responsible persons have, the more they have to rely on sensing EWS.

Applying EWS to pilot projects is by no means trivial for two reasons:

A) A pilot project can be characterized as an instrument to uncover problems in the operational feasibility [21]. Thus the appearance of some EWS may be a justified output, particularly when the actual innovation is being tested (i.e. the main part of the project)

B) As the innovation is untested, crises are much more likely than in a routine IT-project and their causes may vary significantly.

Therefore, those EWS are most valuable for pilot projects that can be observed in the first 20 percent of the project duration (i.e. the typical project ramp-up phase). In this phase, risks relating to the social subsystem and the project management subsystem are more relevant than risks relating to the technical subsystem [23].

3. Methodology

This paper describes an interpretative case study [25] at the end of an action design research project [22]. The authors held leading roles in the research project based on the action design theory, but withdrew from the driving seat before starting the interpretative case study. In interpretative case studies researchers collect the interpretations of the main actors and interpret them. An interpretative case study was chosen, because we aimed to get an in-depth understanding of how actors made sense of their actions and what it meant for them.

Two of the authors plus one senior research assistant collected and coded data using two methods:

1. During the last six months of the project, they took notes during and after major project meetings and after critical incidents. They captured information on activities and opinions of major stakeholders of the project. As it was not clear during this time whether the pilot system would succeed or not, they focused on information that could shed light on the outcome of the project.

2. At the very end of the project they interviewed five project participants from the public administration resulting in five interviews. Those five interviews were recorded, transcribed and coded.

The resulting raw data was jointly interpreted by two of the authors and the senior research assistants in several group meetings.

4. Results

4.1. Case Context

From 2012-2015 the authors were engaged in an Action Design Research project together with a major German city. Building on prior research [17] [19] [20] [18] in several iterations, a software to support citizen advisory services was developed and tested [5] [4] The final system was well accepted by both the participating advisors and citizens [4]. Thus we were able to move on from the proof-of-value phase to the proof-of-use phase [14] It was decided to roll out the CAG (=Citizens Advice Giving) pilot system to several citizens' advice bureaux to test the operational and organizational feasibility. Important tasks in this phase were internal marketing, defining how to offer the service, setting up the technical and organizational service infrastructure, creating an appropriate incentive system and training advisors for their qualifications. At this stage the participating researchers handed over the overall responsibility for the project to the participating project city members (this hand-over had been planned from the beginning). The researchers remained as consultants and observers and giving technical support. After six months the pilot phase was terminated without ever having really been started. It was obvious to the observers that

most of the city personnel obstructed the project, but due to a lack of hard data we can only speculate why this was the case. Laura[2], the departmental head responsible, was not sufficiently qualified to lead the organizational change and was afraid that this would become obvious. The supporting senior project member, Martha, was a typical uncommitted follower who held back her commitment until it was clear that the endeavour was a success. Marc, the organizational change agent, was the only active supporter but he had been entrenched in a fight with Laura since she had replaced him as the departmental head. Sam, the divisional head, knew about this conflict and therefore insisted that Laura should lead the organizational change. And the technician Tom did not have sufficient time.

While we can only speculate on the underlying motives of the actors, we could collect and analyse data on their patterns of obstructive behaviour and their justifications.

4.2. Patterns of obstructive behavior

The fundamental strategy was to do nothing at all and to ignore the requirements for the innovation project. This tactical distinctive coping behavior is called defensive avoidance [24] and can be observed in two action patterns: delaying actions and the denial of responsibility.

A) Delaying actions

In order to support the management of project scope, time and cost, working packages including time lines, quality requirements and resources were assigned to the project members. In regular jour fixe the achievement of the given tasks were discussed and checked. The arguments used by the project members to justify their inactivity can be categorized in the passive and active delaying actions:

Passive (hidden) delaying actions: They said e.g. "I had no time." (Linda) or "The beat is too fast. The time is too short so there is no way to establish the citizens' advice at short notice." (Linda) or they argue based on unspoken rules and regulations, as well as norms such as "Daily business comes first then project business."(Linda) The arguments end up with statements like "I tell them … and then I focus on my job." (Marc). Using all this kind of statements the project members tried to convince us that they couldn't do anything at all. At the same time they denied being responsible for their inactivity and tried to justify it with the current circumstances.

Active delaying actions*:* If passive delaying actions were impossible because they were answerable to the higher authority for their actions (accountability), they actively delayed the tasks e.g. Laura gave the instruction to all of her citizens' advisors to document the reasons why citizens refused to be advised. Later she used the documentation to justify her inactivity instead of analyzing it to improve e.g. the marketing or the way in which the new service was offered. Another tactic was to involve related departments in fulfilling the task given e.g. with the statement "All marketing activities have to be authorized." (Martha) so that our marketing activities had to be stopped. In the following weeks she argued that she couldn't do anything at all because the department responsible didn't answer her emails or didn't call her back. So the citizens knew nothing about the new service offered when they came to the citizens' advice bureau to change their address in their passports.

[2] We use Pseudonyms for all involved persons.

B) Denial of responsibility:

Personnel accountability was an underlying theme of all statements and actions which went along with the actions described. The public officials refused to be accountable. If they were asked about their actions or their non-actions, their justification showed the following patterns:

***Outside observer*:** The public officials tried to distance themselves by using statements which would be used by outsiders e.g. "They let you go to the wall." (Marc) or „I would say, because I was not project manager of this phase." (Marc).

Non-accountable-role: Statements expressed indirectly or directly like "I never did something like that because my team leader Mrs. XY is responsible for my new employees." or "I can't see me doing that." (Laura) were often used to justify the lack of commitment or knowledge. This was accompanied by an active or passive arrangement of non-accountability e.g. "My people are allowed to decide for themselves." (Laura). She passed the decision on to one of the employees without any information about the background, the current circumstances or the consequences.

Camouflage tactics: The project members refused to reveal documents etc. which allowed the transparency and traceability of actions. They strove to hide or to disguise their actions, decisions or instructions to their employees to achieve a maximum of intransparency and untraceability e.g. they told us that they had sent an email with all the necessary information to all of their employees, but they refused to reveal the email or to send it via cc to all the project members. Additionally they refused to let externals talk to their employees and they refused to talk about specific subjects with externals.

Hiding deep in the masses: This phenomenon was often used with statements like "The department decided" or in involving people or other departments which helped to hold the line. This behaviour was chosen to enable them to hide among or behind others.

The unknown third party/person: The last piece in the jigsaw of the denial tactics was the "unknown third party/person" who is not there but is still a part of the project. e.g. "The citizens don't want this." was a statement which was often used but nobody had asked "the citizen" about his/her wishes or opinions.

4.3. Justification patterns

The patterns of obstructive behaviour were justified by three major themes and can therefore be categorized by them.

Insisting on line authority: One characteristic in projects is interdisciplinary cooperation within one or several departments. The project leader normally is the person with the most experience in project management or one of the senior members. Project leaders are responsible for a seamless cooperation and collaboration within the project team, the achievement of the set targets etc. Therefore they have the obligation and the competences to give instructions and feedback, to supervise project work and decide about the next step, to change project members if necessary or to change the direction taken. Their competences are limited to the project so that they can't interfere with the line and staff organization. Considering our case study we observed that the given line organization was mirrored to organize the project work. This ended in a stalemate. The project member Laura, who was boss of the citizens' advice bureaux, was therefore the project leader

during the pilot phase. The project member Marc, who had initiated the project, was only responsible for the IT-part of the innovation project. When it came to the question of marketing, Marc was not allowed to do anything, even if he noticed that something was going wrong and addressed it in the project team because Laura was project leader and refused to give him the competences whenever his work involved her department. Therefore, he withheld his commitment, keeping within the set boundaries and not offending Laura. He stated "… now I can't help anymore."

Another example was inefficient delegation. Mike, the young technician, was responsible for a working package without any information about the situation. After a while he said "… It took a long time to gather all the necessary bits and pieces about the circumstances. After about three months I finally knew that Anna (citizens' advisor in the department for foreigners) was not part of our department … it was kind of prodding in a pea-souper."

Insufficient hand-over of responsibility: To keep projects going during project members' vacations, it is normal to have an interim project member or to pass tasks round within the project team. In our case study the missing team members assigned a member of the line organization to be the interim member. This was positive because they knew all about the daily business and the circumstances of the department. The negative side was the fact that they were not involved in the project and therefore had second-hand information which was actually little or no knowledge about the project, its requirements or its necessities. As soon as they had to substitute the project member the project was slowed down. They then argued that they had no, or only a little, information with statements like "This part – I've never seen that … it is almost embarrassing" or in the case of disinterest they said "I can't say anything. I had no target."

Being "economic" – protection of resources: If working packages were assigned to the project members they would need resources to guarantee or to produce the expected results and therefore hit the desired target. The project members, which at the same time were departmental heads, tried to minimize or to avoid time, effort and costs. They did this to protect their own time and efforts (self-protection) and that of their departmental staff (protection of others). Doing this they often argued that their people were allowed to decide if they wanted to do the necessary tasks or not. This went along with statements like "… we attach a certain value to voluntary work." (Laura) Other statements were „We noticed that it takes too much time and effort to key in all the information needed for this target group." (Laura) or "… we do this without spending too much time or energy…" or "… we did it because *you* wanted us to do it." or "Then we did it because someone had to do it."

5. Discussion

Our study offers three contributions: 1. We demonstrate to employees in the public administration how to best obstruct an E-Government project. 2. We identify early warning signs for E-Government pilots and 3. We demonstrate the need for developing an appropriate culture and structures for E-Government pilots. We regard the first contribution as somewhat ironic and therefore concentrate on the latter ones.

Early warning signs: Obstructive behaviour and their justification can be observed and therefore are good candidates for early warning signs. Both patterns relating to delaying actions and denial of responsibility are related to particular traits of public administration: Public agencies are rule-based systems [4] and deliberate delays are far more accepted instruments than in the private sector,

especially if there is no real stake (as in pilot projects). And public administrations lay more emphasis on a clear separation of responsibilities.

The same holds true for the justification: While commercial companies typically have economical discussions *before* the pilot start or *after* the pilot (when discussing the outcome), in the CAG-pilot economic discussion were made *during* the project. While networked decentralized organizational structures become increasingly common in the private sector [15], strict line management is still unquestioned in the public sector. Successful hand-over of responsibilities mainly relies on the good will of the actors involved.

Thus, to our knowledge, for the first time we have uncovered EWS for pilot projects that are specific to the public administration: Purposeful delays and denial of responsibilities justified by insisting on established organizational rules and spontaneous economic discussions.

What does this mean for responsible people? We propose two measures:

1. Before the actual pilot starts, the attitude of the stakeholders should be tested in a pre-pilot, e.g. using only a very small subset of the functionality. This instrument uses the provisional nature of pilot projects to establish transparency of their feasibility.

2. Responsible project managers should continuously screen pilot project stakeholders' behaviour for EWS. This can be done by adapting established management instruments for stakeholder analysis [25].

Appropriate pilot project culture and structures: If a public administration accepts the necessity for innovations (and piloting them) it should not only provide responsible project managers with instruments to detect and repair counter-productive behaviour but it should also improve the innovation-readiness of the whole administration. The most important (and difficult) aspect is the organizational culture. A pilot project requires a different "mode" of work with a different value system and different norms for acceptable behaviour: Distancing yourself and operating like a wheel in a large machinery is good for routine work because it guarantees égalité and predictability of legal decisions. However it is bad in pilot project when distance leads to denial of responsibility and ultimately prevents learning. Denial of responsibility is easy in pilot projects: The typical first question "Are fundamental risks to be expected if I don't change my attitude?" will most of the time lead to the answer "NO", because a pilot system is not daily work. Additionally public employees have already learned that their behaviour is likely to be accepted if they stick to given laws, rules and norms as well as set organizational boundaries and competences. The "NO" also implies that the innovation is slowed down or even stopped and the hidden goal for the public officials to prevent innovation is reached. If the first question does lead to a "YES" because of incentives and pressure from internal or external factors, then they start to slow down the working process by pretending to be active while using the characteristics of administrative organizational structures and culture which lead to the pathologies according to Hormons' Accountability Paradox.

Instead of applying operational pressure, we rather propose a "pilot project culture": This starts with the senior administrative officials (who typically are the pilot project sponsors). On the one hand, they should not promote a pilot project prematurely as a success and push it into operations; pilot projects are far too risky for that and they would loose credibility. On the other hand the openness of the outcome should not entice them to a wait-and-see attitude. Rather, they should insist that the

participating actors take advantage of the opportunities to learn. Practiced in this manner, top management support is as much needed and beneficial as in other IT projects.

A pilot project culture only comes to life if it is practiced regularly. Thus organizations should prepare themselves for the infrequent larger pilots through more frequent smaller trials, e.g. piloting small improvements of IT tools or small organizational change. In those "micro-pilots" appropriate behaviour can be incentivized and inappropriate behaviour sanctioned. Our research contributes to establishing a pilot project culture by clearly identifying patterns of undesired behaviour and their justifications. We showed that they are deeply engrained in public administration and not peculiar to any specific E-Government project.

A pilot project culture requires the implementation of an appropriate project organization. All observed justifications for inappropriate behaviour boil down to a complete ignorance of project structures. Project structures clashed with the organizational hierarchical structures and are dominated by them to the point that actors stopped project progress by insisting on working within their traditional line of authority. The actors ignored the dynamic nature of project knowledge (in contrast to the static nature of operational knowledge) and thus the hand-over of responsibility did not work. And they ignored the fact that projects have their own budget by frequently questioning the operational economy of the project. Issues of IT-project management are well-known in research and practice. However, the complete lack of established project practice in public administration came as a surprise to us. Thus we call for further research on project practice in public organizations and propose to frame the above mentioned micro-pilots as projects. Thus project management (and work package management) skills can be learnt and embedded in a public organization.

6. Conclusions and Limitations

Pilot projects are a means of learning whether the promises of an E-Government-innovation hold true. Innovations are risky; learning is hard work and requires both sufficient prior knowledge and a sufficient learning capacity. In this paper we showed that in the case of the CAG-pilot the public administration was ill-prepared for the risks and the learning requirements of the pilot. This offered the opportunity to study obstructive behaviour that ultimately lead to the unsuccessful termination of the pilot. We propose to use the observed behavioural patterns and their justifications as early warning signs for E-Government pilot projects. We furthermore use the results to propose a pilot project culture and - as a means of implementing it - micro pilots to train behaviour and how to work in a pilot project context.

There are some limitations to our research. As in any interpretative case study, the observed case may not appropriately represent the public sector outside Germany or even inside Germany. This trade-off between deep insights vs. external validity is typical for case studies. As we find support in the literature for many foundational phenomena and as all three authors have extensive experience in prior E-Government pilot projects, we are optimistic that we do not only report on a singular case, but we do not have scientific means to prove that. A second limitation refers to the authors' role in the project. While on purpose the two active authors did not sit in the driving seat of the pilot project they may have framed the participants in the prior phases of the project in a way that heavily influenced the pilot projects outcome. This again is a trade-off between the deep insight that a researcher receives when he is personally involved with the project's actors and his or her neutrality when gathering, coding and interpreting data. Thus we call for further research on E-Government pilot projects to validate our results and encourage researchers and practitioners to also

report their failures. In this way, we can improve the way we use the valuable instrument of pilot projects in the public sector and thus improve the E-Government innovation uptake.

7. References

[1] CLAVER, E.; LLOPIS, J.; GASCóM, José L.; Molina, H., Conca, F. J.: Public Administration: From Bureaucratic culture to citizen-oriented culture. International Journal of Public Sector Management Vol. 12, Iss. 5, 455–464 (1999)

[2] DEAL, T.; KENNEDY, A.: Unternehmenserfolg durch Unternehmenskultur, Bonn, Bad Godesberg, Rentrop (1987)

[3] GIESBRECHT, T.; SCHENK, B.; SCHWABE, G: Empowering front office employees with counseling affordances. Transforming Government, Vol. 9 (4), Emerald Group Publishing Limited, p. 517ff. (2015)

[4] GIESBRECHT, T.; SCHENK, B.; SCHWABE, G.: Learning with affordances: The case of citizens' advice services. In: Twenty Second European Conference on Information Systems 2014-06-09 (2014)

[5] GIESBRECHT, T., SCHOLL, H. J.; SCHWABE, G.: Smart Advisors in the Front Office: Designing employee-Empowering and Citizen-centric services. Rev. Government Information Quarterly, 30(4), pp. 377-386 (2015)

[6] HAUSCHILDT, J.: Widerstand gegen Innovationen - destruktiv oder konstruktiv?, in: Zeitschrift für Betriebswirtschaft, Ergänzungsheft 2, 69, 1-21 (1999)

[7] HAVELKA, D., RAJKUMAR, T. M.: Using the troubled project recovery framework: problem recognition and decision to recover. E-Service Journal 5.1, 43-73 (2006)

[8] HILL, H.: Von Innovationsmanagement und Management der Unsicherheit zur Zukunftsfähigen Verwaltung. Verwaltung & Management, 1/2007, 17. Jg.; 1-7 (2011).

[9] HINZ, E.: Neue Verwaltungssteuerung und Mitarbeiterführung. Kontextsteuerung zur leitbildgerechten und leistungssteigernden Komplettierung des Managementwandels in NPM-Systemen. München, Meiring; 1. Auflage (2012)

[10] JANIS, I. L.; MANN, L.: Decision making: A psychological analysis of conflict, choice, and commitment. New York, NY, US: Free Press Decision making: A psychological analysis of conflict, choice, and commitment (1977)

[11] KAPPELMAN, L. A.; MCKEEMAN, R.; ZHAN, L.: Early Waring Signs of IT Project Failure: The Dominant Dozen. Information Systems Management; Fall 2006; 23,4; ABI/Inform Global, 31-36 (2006)

[12] PHILIP, T.: Early warning signs of failures in offshore outsourced software development projects at the team level, University of Zurich, Faculty of Economics, Dissertation (2013)

[13] MERTENS, P.: Fehlschläge bei IT-Großprojekten der Öffentlichen Verwaltung-ein Beitrag zur Misserfolgsforschung in der Wirtschaftsinformatik. Multikonferenz Wirtschaftsinformatik. Vol. 2. (2008)

[14] NUNAMAKER Jr, J. F., et al.: The Last Research Mile: Achieving Both Rigor and Relevance in Information Systems Research. Journal of Management Information Systems 32.3; 10-47 (2015)

[15] RICHTER, A. (ed.): Vernetzte Organisation. Walter de Gruyter GmbH & Co KG, München (2014)

[16] ROMZEK, B.: Dynamics of public sector accountability in an era of reform International Review of Administrative Sciences, SAGE Publications, London, Thousand Oaks, CA and New Delhi, Vol. 66, 21–44; (2000)

[17] SCHENK, B.; SCHWABE, G.: Design IT-gestützter kooperativer Bürger-Beratung. In: Multikonferenz Wirtschaftsinformatik MKWI 2010, Universitätsverlag Göttingen, 2010-02-23 (2010)

[18] SCHENK, B.; SCHWABE G.: Bürgerservices vor Ort. In: Schwabe (ed.): Bürgerservices: Grundlagen, Ausprägungen, Gestaltung, Potenziale. Edition Sigma, Berlin, 139 – 160 (2011)

[19] SCHWABE G.; BRETSCHER, C.; SCHENK, B.: Designing for light-weight collaboration: the case of interactive citizens' advisory services. In: DESRIST Conference, Springer Verlag, 2010-06-04, (2010)

[20] SCHWABE, G.; SCHENK, B.; BRETSCHER, C.: Enabling advisors and citizens through Citizens' Advice 2.0. In: 14th Annual Conference of the International Research Society for Public Management (IRSPM), 2010-04-07 (2010)

[21] SEIFERT, E. K.: Einführung. Joseph Alois Schumpeter: Zu Person und Werk in: Joseph A. Schumpeter: Kapitalismus, Sozialismus und Demokratie. Einführung. Von Eberhard K. Seifert, 7. erweiterte Auflage, Tübingen/Basel, 3-14 (1993)

[22] SEIN, M. K., et al.: Action Design Research, Management Information Systems Quarterly 35:1 (2011)

[23] THOM, N.: Innovationsbereitschaft, Innovationsfähigkeit und Innovationswiderstand – Erfahrungen aus dem Schweizer Umfeld, in : Hilgers, D./Schauer, R./Thom, N.(Hrsg.): Innovative Verwaltung. Innovationsmanagement als Instrument von Verwaltungsreformen. Internationales Forschungscolloquium „Public Management" an der Johannes Kepler Universität Linz. Eine Dokumentation, Linz, Donau, 15-38 (2011)

[24] WALTER, A.: Das Unbehagen in der Verwaltung. Warum der öffentliche Dienst denkende Mitarbeiter braucht. Edition sigma, Berlin (2011)

[25] WALSHAM, G.: Interpretive vase studies in IS research. Nature and method. European Journal of Information Systems, 6, 69-90 (1995)

[26] WARD, J.; DANIEL, E.: Benefits Management: Delivering Value from IS and IT Investments. John Wiley and Sons, 2010

[27] ZWIKAEL, O.: Top management involvement in project management. A cross country study of the software industry. International Journal of Managing Projects in Business. 1, 4, 498 (2008)

DIGITALISATION VS. INFORMATIZATION: DIFFERENT APPROACHES TO GOVERNANCE TRANSFORMATION

Alois Paulin[1]

DOI: 10.24989/ocg.v331.21

Abstract

The twentieth century brought humanity radically new knowledge in form of electronics, informatics, and telecommunication technologies, which gave rise to cyberspace as a channel for data exchange, data storage, and as an enabler of new approaches to steering and controlling real-world systems. Thus-created new opportunities have been successfully deployed for the automation of processes in areas such as production, service provision, data exchange, navigation, logistics, etc., or for creating new possibilities through concepts of virtualisation, respectively. While this has led to radical transformations of paradigms in industry and free market service provision, the systems that make up modern states have been broadly spared of disruption by these technologies. Behind this backdrop, this contribution aims to discuss the differences between digitalization and informatization as two differing approaches to system transformation. The discussion is set in the context of societal governance, where digitalization is the main approach to modernisation. The focus on digitalisation and the lack of progress towards informatization in this field of interest is criticized, and the advantages of informatization are brought to attention.

1. Introduction

Contemporary buzzwords containing attributes such as "Smart-*", "*-4.0", "Cyber-Physical", "intelligent", etc., which dominate discussions in areas of sales, marketing, and consultancy (and as such slop over to scholarly deliberations as well) have superseded a previous generation of buzzwords characterized by attributes such as "e-*" / "electronic", or "digital". Although none of these terms are clear technical terms, the swap of terminology nevertheless reflects a change of the underlying matters at stake and is justified by existing advances in technology.

Amongst these buzzwords, the "4.0" suffix stands out in a special way. The suffix emerged as part of "Industrie 4.0", a high-tech strategy document of the German federal government from 2013 [6]. The objective of that document was to provide a future vision of industry by the year 2025, taking emerging trends and advances in Internet technology as a point of departure. In that document, "Industry 4.0" stands for the use of Cyber-Physical Systems (CPS) for industrial manufacturing, whereby a CPS according that document is a network of embedded computers, which can be used to individually steer manufacturing processes. CPS there is explicitly used as a synonym for the Internet of Things (IoT) [6]. In a nutshell: the German Federal Government through this document conveyed a vision that the Internet of Things will lead to a fourth industrial revolution (hence, the "4.0"), which will catapult German and the Western industry again miles ahead of the emancipated Asian competition.

[1] Facult of Organisation Studies in Novo mesto, Novo mesto, Slovenia

The "4.0" buzz-suffix was soon picked up by other domains: Health 4.0 [31], Public Administration 4.0 [27], are two examples that have been taken serious enough to enter the scholarly discourse. This led scholars to re-adjust the "4.0" suffix in the context of the respective domains. While originally Industry 4.0 refers to an emerging 4th industrial revolution (the first one triggered by steam power, 2nd: introduction of the conveyor belt, 3rd: electronics, 4th: digitalization), the "4.0" in other domains refers to a different kind of change. In Public Administration the "4.0" is interpreted as a futuristic administration that is fully automated, transparent, and non-political [27], while the "4.0" in Health refers to a future evolution of public healthcare systems where harvesting and governance of personal data plays a decisive role [18]. What is common to the use of "4.0" throughout these disciplines is that it refers to a novel generation in the respective domain.

This article aims to unravel the buzzwords and describe the underlying novelty of the switch to a new set of terminology. Section 2 shall describe the four generations of controlling structure, to interpret how the new terms came to be. There, the difference between *digitalization* and *informatization* shall be explained. Section 3 will discuss how *digitalization* and *informatization* translate to technology applied to control and deliver public governance. Section 4 will conclude with a discussion on the implications of *informatization* on public governance and outline the challenges for the scholarly debate.

2. Understanding the four generations of controlling structure

In order to understand the potential effects technology can have on industry, commerce, society, and societal governance, one must develop an understanding for the respective characteristics of changed approaches to technology. For this purpose, the "four-revolutions" model as popularly used in history and economics however is insufficient: While the four industrial revolutions (the last one yet waiting to happen!) may serve as milestones to segment evolution of society into characteristic areas of time in which a number of factors triggered a chain reaction of memorable societal changes (de-feudalisation, urbanisation, shuffles in economic and political power, changes in moral and societal values, …), they focus on fashions of production (e.g. conveyor belt and automation as facilitators of mass production), availability of new technical systems (e.g. cars, railroads, telecommunications, bicycles), or materials (iron, petroleum, paper) [29], which are categories too broad to identify technologies that can trigger further transformations.

An approach to identify technology triggers is the generations model [18, 19]. In that model, the focus of observation is the approach to controlling structured processes of work / production, where four distinct generations are identified: mechanization, automation, computerization / digitalization, and informatization. Unlike the revolutions model, which deals with historic time spans, the generations model focuses on the ripeness of a specific domain, and its influence on fostering progress in others.

The 1st generation (mechanization) refers to the introduction of machines in work processes. An example for this step is the 18th-century invention of the Jacquard loom as a game-changer in the production of woven fabric [12]. The Jacquard loom was a mechanical, man-powered device, which structured the process of weaving, and used a system of punch-cards to describe the weaving pattern. Other examples of structured, mechanized systems, are the late 18th-century threshing machine, or the 19th-century typewriter. Characteristic for the first generation is thus the transformation of previously unstructured work (like weaving, threshing, or writing) into a well-structured, mechanized (i.e., conducted by machines) process, with manual labour used to progress through the individual stages of the process.

The second generation (automation) is then characterized by the introduction of power to *automate* previously structured and mechanized processes. Instead of the individual stages of the process being moved manually, the process is now progressed automatically stage-by-stage without manual intervention. The 18th-century steam engine, the 19th-century electric Jacquard loom, or the late 19th-century Benz motor car, are all examples of automated machines belonging to the second generation of structure control, and so are 16th-century mechanical watches. The given examples, most of which coincide with the society-transforming industrial revolutions, must however not be misunderstood: automation of machines and devices has been known long before the renaissance of Western high civilisation [2]. Furthermore, automation is not limited to a specific type of power provided to the system – the spring, which powers a watch, the water stream that powered mechanical theatres (cf. [26]), the steam engine and the combustion engine as generators of power, and electricity, are all equally valid sources of power that enable automation.

In the 3rd (computerization & digitalization) and 4th (informatization) generation, control of structure and processes relies on electronics and the possibilities derived from that. Following two sections shall deal with their characteristics and implications in more detail.

2.1. The third generation: computerization & digitalization

The 20th-century brought the digital computer (cf. the 1920ies Lehmer sieve as an early non-electronic digital computer), and electronics as a radical novelty to human knowledge. From these soon first computerized systems for industrial production emerged, which used digital computers and electronics for controlling process flows. Electronics as a way to control systems can be steered by software, which in turn enables a never before possible amount of precision and new possibilities to control a technical system.

Software enables a type of control that goes beyond mere automation: Zuboff's 1980ies book *In the Age of the Smart Machine* describes with fascination how software, which is used to steer processes of computerized machines, keeps in memory the state of the thus steered process, which in turn enables this very same software to act based on knowledge of the state - Zuboff called this ability *informating* [32]. Her use of *informating* thus refers to the inherent context-awareness of systems which have been designed in such way that software not only steers their performance, but also generates, stores, and uses information about the context: *"The programmable controller not only tells the machine what to do – imposing information that guides operation equipment – but also tells what the machine has done – translating the production process and making it visible."* (ibid., p.10)

Zuboff's fascination for the duality of information technology is comprehensible if one takes into account her time, in which a radically novel generation for controlling structured processes emerged. However, from a 21th-century perspective, the fascination has faded away, as software controllers (and their inherent state-awareness) became a normality in engineering and management in the digital age. Zuboff's informated *smart machine,* which not only automates processes of production, as 2nd-generation machines were capable of, but is also aware of its own current state within the context, is thus a machine managed by 3rd-generation controllers, whose primary objective is to *automate* specific processes (such as soldering car parts, harvesting crops, calculating salaries, or counting votes), while the machine's state-awareness enables an unprecedented level of precision and complexity.

The defining characteristic of the 3rd generation of control is thus the use of the *computer* as a device, which processes data, acts upon information, and composes instructions to context-consciously govern the process(es) of the system it controls. This level of control is best called *computerization* – such system is then *computerized*. Typical examples of computerized systems are industrial robots, automotive electronics, computer-steered domestic appliances (fridge, dishwasher, electric stove, air conditioning, …), etc.

Many scholars instead of *computerization* use the semantically largely overlapping, if not fully synonymous term *digitalization*. The crux with these terms is that they lack precision: *digitalization* is frequently used to refer to the use of information and communication technologies for business / administration [11], and also the Oxford English Dictionary (OED) defines it in such way *("The adoption or increase in use of digital or computer technology by an organization, industry, country, etc."* [17]); other sources however use it as a synonym for *digitization* (also Oxford Dictionary of English (ODE) defines it as such), an established technical term referring to the transformation of analogue signals (or real-world items) into a digital representation. On the other hand, *computerization*[2] implies a closer proximity to hardware-controlling software. Accordingly, I suggest following use: electronics in the car and dishwasher make them *computerized* systems, while the use of accounting software makes a business *digitalized*.

2.2. Fourth generation: informatization

Up till the 3rd generation, technical artefacts were designed to control processes for production and processing of goods (e.g. loom, combine harvester), to control administrative processes (e.g. census, accounting), or to steer the functioning of devices (e.g. clock, dishwasher). Up till then, the controller as a steering mechanism was an integral part of the system – i.e., the way the system behaved was determined by the mechanism which was part of the system itself. Thus, in first and second generations of control, the control mechanism and logic was defined by the physical architecture of the system's hardware; the third generation introduced the switch to software, but left the architecture (i.e. its functionality and program flow) of the pre-compiled software determine the functionality of the machine.

The defining novelty of the 4th generation lies in the reliance on the *digital (computer) file* as the descriptor of a system's (or digital object's, respectively) characteristics and state. More specifically, the type of *file* at stake is the type which can be exchanged, shared, edited. While the computer file as a concept to store a system's state is known since the 1950ies, it is only the later evolution of file systems as part of wide-spread computer operating systems, and files in form of standardized, open file types, which made the new generation happen.

The modern computer file constitutes digital objects in their *serialized* – that is, written down in digitally readable structure, form. Computer programmes, which make use of the file, *deserialize* the information and make use of data / information / instructions contained in the file – the way a given file is used, depends finally on the system it is used by. A *file* can then be a composition of graphic elements, a plug-in for a computer program, or a software library that extends functionality of a computer program. A PDF file for example can be composed by a digital artist (and edited by its peers) using desktop publishing software such as Adobe Illustrator – such file will then contain a

[2] OED: "The action or process of computerizing an organization, activity, etc.; the conversion of information, text, etc., into a form which can be stored or processed by computer." [16] – note the proximity to digitization!; ODE: "convert (a system, device, etc.) to be operated by computer: the advantages of computerized accounting."

logical composition of graphics and text, which can be interpreted by other software to instruct display hardware to render the graphical composition on the computer screen. The very same file can then be transferred to a printing software, which will instruct printing hardware to create a tangible instance of the digital graphic. During all stages, the file from this example remains the *original* digital object, which can be created, edited, deserialized, shared, copied, transformed, rendered to a human-perceptible representation, etc. in a potentially indefinite number of ways.

In order to be able to instantly co-work on a file, networked work spaces (computers with the required software) are of advantage, amongst which the file can be shared. The sharing of files that contain virtual compositions (graphics, multimedia, …), software systems / components (executable code), or other types of digital objects, enables the emergence of virtual co-productive communities, which rely on cyberspace as a gathering environment (cf. [24]). This very emergence of *cyberspace* in terms of a dimension for interaction, production, and creation of value (online services, etc.), is another enabler of the 4th generation for controlling structure. Although at the end of the day all interaction in cyberspace is nothing but the exchange of data between terminal equipment, interaction in cyberspace is so different in quality and complexity, that it must be distinguished from plain exchange of signals / data as it occurs in telephone calls or telemetric readings. Foreseeing the upcoming change of quality of information and communication technologies, Nora & Minc in the years of the emerging Internet coined the word *telematics* in their *The Computerization of Society* [28]. Although the word *telematics* (as well as the prefix *tele-*, as in television, or tele-voting) meanwhile went out of fashion, the justification for the then-new word *telematics* is a relevant indicator of substantial change in generation of technology.

The modern file is thus more than a mere representation of a system's state (as the early computer file was), and more than a set of processing instructions (as would be sufficient for purposes of automating and informating a system) – it is a genuine object, which exists natively in its digital form and only when interpreted by software descends from cyberspace to the physical world (in perceptible form as print-outs / products / visualisations / music / movies, …, or actions such as e.g. granted access to resources, movements of robot arms, etc.).

To refer to such 4th-generation system, following vocabulary should be used:

- *Informatizing* (verb) stands for the creation (or conversion) of a system into a form, which crucially relies on digital objects (described through files).

- A system, which crucially relies on digital objects, is *informatized* (attribute).

- *Informatization* refers to the culture of engineering systems, which are *informatized* by design, and thus to the 4th generation as such.

All words, except for *informatization*, I'm hereby coining specifically for the purpose to satisfy the need for demarcating the 4th generation from the 3rd. The word *informatization* is being in popular use already, whereby the OED defines it as *"the adoption of information technology; computerization"* [17]. The crux with this existing semantics however is, that thus a total of three different words (*informatization, digitalization, computerization*) all would stand for vaguely the same – namely the use of an ambiguous mixture of information technology (software), digital computers (software + hardware), and electronics (hardware) in a given context (or their introduction therein). For sake of professional clarity in the use of words, I hereby accordingly

propose to use the terms *informatizing / informatization / informatized* solely in the context of 4th-generation systems as described herein.

2.3. Unravelling the buzzwords

Researchers interested in understanding systems of societal governance, are used to deal with ambiguous semantics: *bureaucracy*, for example, can mean a social class (like *aristocracy* or *clergy*), a type of organisation, the system of public administration, or the administrative procedure (cf. [1] for a rigorous treatise on that). Likewise, *governance* has a myriad of meanings [3], so does *democracy*, and so on. Given this culture of unclearness, it does not surprise if *computerization*, *digitalization*, and *informatization*, all mean kind of the same in popular (and sadly, also in scholarly) discourse – that is: introducing technology to modernise the way business is conducted. In above sections, I undertook the humble attempt to identify semantic differences of these terms and assign them to different situations of use. I consider such differentiation crucial for the advancement of our scholarly field, as only precise terminology can help us properly identify or define challenges and potentials that involve or affect multiple disciplines.

Having clarified the terminology, we can then move to align the buzzwords according to these categories. In the introduction to this article, two groups of terms were identified: “smart”, “4.0”, “cyber-physical”, and “intelligent” belong to one group, which refers to the systems that rely on the 4th-generation of control; the other group are “e”, “electronic” and “digital”. The line of reasoning is as follows: “4.0” as per definition of the ur-document [6] refers to the use of cyber-physical systems; the attributes “smart” and “intelligent” as used in the context of man-made systems (i.e., either technical systems such as smart phones, or systems of organisation such as smart cities) refer to the systems’ reliance on information systems which crucially depend on shared digital objects, have optional network connectivity (to instantly exchange digital objects) and make use of platform systems (software stacks, such as e.g. Windows as operating system, which hosts the graphics software Adobe Illustrator, which can be used as a tool to create and edit graphic compositions stored as PDF files) that provide functionality to create / render / edit / reuse, etc. the digital objects (cf. [8, 30] for a better explanation of “smartness”). Such characteristics of “smart” / “intelligent” / “cyber-physical” systems allow them to be independently extended during run-time beyond the limitations as imposed by the original makers of the system. This very ability to be extended makes them go beyond the limited abilities of systems that would otherwise fall under the 3rd-generation of control.

The second group (“e” / “electronic” / “digital”) denotes systems and software without the ability for co-creation. An electronic / digital system’s functionality is thus limited to providing a specific pre-determined routine. An e-voting system for example is built to register voters, assure integrity and anonymity of the votes, and provide results in the end. Although a modern-day e-voting system will be built using systems and tools that belong to the range of 4th-generation systems, the e-voting system itself remains a 3rd-generation system, since it isn’t enabled for co-creation / extension by its users. The “e” / “electronic” / “digital” thus stands for systems that are “electronic” / “digital” to the extent that they are controlled by software, without being designed to be extended / amended by its tech-savvy users.

3. Transforming governance – digitalization vs. informatization

Radically new possibilities of technology inspired scholars of the 1970-90ies to think about new possibilities enabled by *digitalization* and beyond: Nora & Minc's *telematics* (end-1970ies) describes a transition to *informatization*, enabled by networked computers; Ascott's 1980ies *telematic art* [cf. 28] is a future vision of telematics-enabled co-creation (distributed authorship), where authors would co-create works of art by means of networked robots, even if working thousands of miles away from each other; Zuboff's end-1980ies *informating* [32] describes information systems, which gain *smartness* through their ability to be state-conscious. While these early predecessors of *informatization* already rely on computer networks, co-creation, or computer memory for situation-aware action, they do not take into account yet the computer file / digital objects as the crucial enablers of *informatized* systems.

New possibilities brought by the 20th century, were soon followed by radical transformation of domains such as communication, logistics, publishing, entertainment, retail and advertising, public discourse, and other domains of economy and civilisation. The manifold novelties brought by information and communication technologies over the last decades (Internet, the Web, cellular networks, satellite navigation), enabled by electronics and digital computers, do not need to be explicitly listed for one to understand how significantly the mentioned domains differ in 2017 if compared to 1967, or 1917! What is crucial to understand, is the leap of these domains from *digitalization* and *informatization*: Was the telefax yet a typical 3rd-generation terminal system for transmitting *digitized* letters, the email client is already an informatized system relying on the email as a container of digital objects. Was the GPS system yet a 3rd-generation constellation of man-made celestial objects for calculating one's position on the globe, Google Maps &co. use the Internet and a system of accessible standards for co-creating an *informatized* ecosystem.

3.1. Governance digitalization – a history drag?

While the leap from *digitalization* to *informatization* radically transformed the world we live in, making old cultures and business models die out to leave room for new (think of paper maps vs. modern automotive navigation, phone boots vs. smart phones, physical journals vs. online papers, etc.), it failed to transform the systems of governance, which stuck in the 3rd generation of structure control. Even though politics, public administration, and the judiciary, as the key branches of public governance have undergone a substantial evolution by taking-up use of software to modernize their front- and back-office activities, this evolution has come to a stop at *digitalized* (3rd-generation) systems: Street-level bureaucracies have given way to system-level bureaucracies to transform administrative discretionary power [5, 14], online tools are used as channels for government agencies to receive feedback from citizens [9], and social media as a form of managing public relations [15].

The underlying framework however remains the same: the model of politics, legislation through elected representatives, the model of public revenue and expenditure, the culture of red tape, etc. Stemming from times when officialdom and bureaucracy, democracy and parliamentarianism, the social state and worker's unions, VAT and the fiat monetary system, were radically novel ideas enabled and supported by a society churned up by the transition from agrarian to industrial economy, these established cultures and institutions continue to withstand the possibilities of 4th generation technology.

Existing culture in this domain implies limits, which impact the way technology can be applied. In the domain of public administration, for example, Lenk distinguishes between three types of processes [13]: recurrent and well-structured processes which can be automated on the one side, and individualized decision-making as well as negotiation processes, which can be supported by IT, but not automated, on the other. The first two types of processes have largely been *digitalized* (automated decisions, screen / system level bureaucracy; [cf. 5]), but further pushes for modernization within the limits of *digitalization* lead to controversial ideas and developments such as the use of data mining techniques for analysing the sentiment of the governed subjects. While such ideas (contemporarily promoted using the buzzword Big Data) do not change the established paradigms of societal governance, they bear the immanent risk of preventing the evolution of history (Riedl: "*Geschichtsbremse*" – "*history drag"* [25]) by reinforcing existing power relations of governance systems beyond repair. I've raised the manifold issues of *digitalized* government technology previously [20, 23], pointing out that such technology is costly, unsustainable and discriminative in the worst case, while in the best case the dependency on such systems leads to the emergence of a neo-feudal system in which controllers of the digitalized services have the upper hand.

3.2. Governance informatization

Unlike *digitalization* of governance, governance *informatization* for now exists only on a level of conceptual studies and proof-of-concept experiments. Outlined below are three concepts, which base on the paradigm of *informatization* – i.e. embrace the principles of networked co-creation of open, accessible files as a matter of controlling systems of public governance. These concepts are Governance Informatization [22], Liquid Democracy [21], and the Quantum Budget.

Governance Informatization

Initially termed "self-service government" [22], then "informating governance" [19], the concept of Governance Informatization (GI) bases on the assumption that a system of distributed files containing jurally relevant facts (such as certificates of education, driving permits, etc.) could serve as a source to determine one's eligibilities in a given (jurally relevant) situation. The principles of GI are inspired by Jellinek's systemisation of jural eligibilities into the system of subjective public rights [10], which describes one's position in a jurally relevant situation through the involved individuals' jural status. This system would allow subjects to co-create governance by altering the contained data, whereby access to data would be regulated through a dynamic fine-grained access control system.

Liquid Democracy

Liquid Democracy (LD) is a way of making collaborative decisions through a system, in which interpersonal relations of trust are digitally stored, and thus reflect an ever-changing (hence, "liquid") network, through which communal decisions in matters such as legislation, appointments of representatives, public spending, etc., can be made [21]. From a perspective of democratic theory, this way of collaborative decision making has been found superior to other forms of direct democracy [4]. The concept of LD is complementing Governance Informatization, in terms that it allows the engineering of a general-purpose technical system able to endure future changes of the hosted real-world systems of governance [21].

Quantum Budget

With the combined power of Governance Informatization and Liquid Democracy, a new approach to public revenue and public spending can be realized, where taxes would not be transferred to a central authority, but instead remain in the possession, although outside of control of taxpayers. Taxes owed by a subject to the community would instead be automatically (i.e., formula-based – cf. the key-lock paradigm from [22]) locked according to valid legislation, and would be used for purposes of public funding when required. This would open new ways to look at taxation and public funding, which however yet need to be further explored.

4. Discussion – a new spectre that haunts the world?

Expecting institutions of public governance to give up their rubber stamps in order to voluntarily give way to new paradigms of governing the common good, would be naïve – it doesn't fit the lifecycle of these bureaus, as Downs described it [7]: bureaus (as do other types of organisations such as churches, corporations, etc.) follow the ambition to expand their territory and influence, take over other bureaus and their resources, and increase their revenue. For satisfying these ambitions, *digitalization* is a suiting approach, as it positively addresses performance in terms of effectiveness, efficiency, and sometimes economy, without meddling with the overall architecture of institutions that make up public governance. Digitalization thus turns into a welcomed tool to demonstrate modernization through technology, without endangering the hegemony of the bureaucracy.

Informatization, on the other hand, is defined amongst others by its reliance on co-creation, which implies accessible (open, transparent) files and communication protocols, and comes with an inherent attitude that warmly embraces self-service – an important added value of *informatization* is thus the elimination of the middle-man. To this end, *informatizing* public governance would openly challenge strongly rooted models and narratives of public governance, which crucially rely on a service-based paradigm of operation (officers to issue permits, municipal commissions to decide on public funding, electoral committees to govern elections, legislative assemblies to pass laws, etc.).

Was it yet *socialism*, which haunted the entrenched European aristocratic and cleric establishment during the last decades of the second industrial revolution, it is now the pressing *informatization* that calls for transformation in all segments of society. What both spectres of change have in common, is the hope for new opportunities for emerging generations whose appetites the entrenched systems fail(ed) to satisfy. Prominent proponents of organizations, which embraced the new opportunities of *informatization* with success, are corporate giants such as Google, Uber, or Tencent, and non-profit social service providers such as Mozilla, the W3C, Wikimedia, or Wikileaks.

Gathering knowledge for building towards the transition to actually-existing informatized governance is the duty of science and engineering. This task is to be approached by developing theories, concepts, models, and laboratory experiments, which further explore the implications and potentials of *governance informatization* as the next step in transforming governance to a level beyond bureaucracy.

5. References

[1] ALBROW, M. 1970. *Bureaucracy*. Macmillan.

[2] BANŪ-MŪSĀ, AḤMAD IBN MŪSÁ IBN ŠĀKIR and ḤASAN IBN MŪSÁ IBN ŠĀKIR 1979. *The book of ingenious devices*. Reidel.

[3] BEVIR, M. 2009. *Key concepts in governance*. SAGE.

[4] BLUM, C. and ZUBER, C. I. 2016. Liquid Democracy: Potentials, Problems, and Perspectives: Liquid Democracy. *Journal of Political Philosophy*. 24, 2 (Jun. 2016), 162–182.

[5] BOVENS, M. and ZOURIDIS, S. 2002. From Street- Level to System- Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control. *Public Administration Review*. 62, 2 (Dec. 2002), 174–184.

[6] BUNDESMINISTERIUM FÜR BILDUNG UND FORSCHUNG 2013. Zukunftsbild "Industrie 4.0."

[7] DOWNS, A. 1967. *Inside bureaucracy*. Little, Brown.

[8] GRETZEL, U., WERTHNER, H., KOO, C. and LAMSFUS, C. 2015. Conceptual foundations for understanding smart tourism ecosystems. *Computers in Human Behavior*. 50, (Sep. 2015), 558–563.

[9] HARTMANN, S., MAINKA, A. and STOCK, W. G. 2017. Citizen Relationship Management in Local Governments: The Potential of 311 for Public Service Delivery. *Beyond Bureaucracy*. A.A. Paulin, L.G. Anthopoulos, and C.G. Reddick, eds. Springer International Publishing. 337–353.

[10] JELLINEK, G. 1905. *System der subjektiven öffentlichen Rechte [System of subjective public rights]*. JCB Mohr (P. Siebeck).

[11] KATSIKAS, S. K. and GRITZALIS, S. 2017. Digitalization in Greece: State of Play, Barriers, Challenges, Solutions. *Beyond Bureaucracy*. A.A. Paulin, L.G. Anthopoulos, and C.G. Reddick, eds. Springer International Publishing. 355–375.

[12] KEATS, J. 2009. The Mechanical Loom. *Scientific American*. (Aug. 2009).

[13] LENK, K. 2012. The Nuts and Bolts of Administrative Action in an Information Age. *Innovation and the Public Sector*. (2012), 221–234.

[14] MAKOWSKI, G. 2017. From Weber to the Web… Can ICT Reduce Bureaucratic Corruption? *Beyond Bureaucracy*. A.A. Paulin, L.G. Anthopoulos, and C.G. Reddick, eds. Springer International Publishing. 291–312.

[15] MAMBREY, P. and DÖRR, R. 2011. Local Government and Social Networking Technologies in Germany: The Example of Twitter. *Proceedings of the International Conference for E-Democracy and Open Government* (Krems, 2011).

[16] OXFORD ENGLISH DICTIONARY 2010. computerization, n. *Oxford English Dictionary*.

[17] OXFORD ENGLISH DICTIONARY 2010. digitalization, n.2. *Oxford English Dictionary*.

[18] PAULIN, A. 2017. Data Traffic Forecast in Health 4.0. *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*. C. Thuemmler and C. Bai, eds. Springer International Publishing. 39–60.

[19] PAULIN, A. 2016. Informating Smart Cities Governance? Let Us First Understand the Atoms! *Journal of the Knowledge Economy*. (Apr. 2016).

[20] PAULIN, A. 2016. Technological Ecosystems' Role in Preventing Neo- Feudalism in Smart-City Informatization. *Proceedings of the 25th International Conference on World Wide Web Companion* (Montreal, Canada, Apr. 2016).

[21] PAULIN, A. 2014. Through Liquid Democracy to Sustainable Non-Bureaucratic Government - Harnessing the Power of ICTs for a novel form of Digital Government. *eJournal of eDemocracy and Open Government*. 6, 2 (2014).

[22] PAULIN, A. 2013. Towards Self-Service Government - A Study on the Computability of Legal Eligibilities. *Journal of Universal Computer Science*. 19, 12 (Jun. 2013), 1761–1791.

[23] PAULIN, A. 2015. Twenty Years After the Hype: Is e-Government doomed? Findings from Slovenia. *International Journal of Public Administration in the Digital Age*. 2, 2 (32 2015), 1–21.

[24] RAYMOND, E. S. 1999. *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. O'Reilly Media.

[25] RIEDL, R. 2016. Big Data – schnell erklärt. *SocietyByte - Wissenschaftsmagazin des BFH-Zentrums Digital Society*.

[26] SCHABER, W. 2004. *Hellbrunn Schloss, Park und Wasserspiele*. Schloss Hellbrunn.

[27] SCHUPPAN, T. and KÖHL, S. 2016. Verwaltung 4.0: Modernisierungsrelevant oder alter Wein in neuen Schläuchen? *Verwaltung & Management*. 22, 1 (2016), 27–33.

[28] SHANKEN, E. A. 2000. Tele-Agency: Telematics, Telerobotics, and the Art of Meaning. *Art Journal*. 59, 2 (2000), 64.

[29] SMIL, V. 2005. *Creating the Twentieth Century*. Oxford University Press.

[30] SÖDERSTRÖM, O., PAASCHE, T. and KLAUSER, F. 2014. Smart cities as corporate storytelling. *City*. 18, 3 (May 2014), 307–320.

[31] THUEMMLER, C. and BAI, C. eds. 2017. *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*. Springer International Publishing.

[32] ZUBOFF, S. 1988. *In the age of the smart machine: the future of work and power*. Basic Books.

Workshop on Smart Cities, Council of Europe III

THE ROLE OF INTERNET OF THINGS IN DEVELOPING SMART CITIES

Andreea-Maria Tirziu[1] and Catalin Vrabie[2]

DOI: 10.24989/ocg.v331.22

Abstract

A main characteristic of smart cities is the use of information and communications technology in all aspects of city life. In this regard, Internet of Things (IoT) is a core element in the process of developing communities "ruled" by an improved communication, better understanding and wait times decrease. This paper aims to present the ways in which IoT networks and services can contribute to develop smart cities, giving as example various cities that have implemented this concept. The methodology used to carry out this research is both bibliographic – opting here to study the work of specialists in the field, authors from Romania and abroad, and empirical – formed by a case study on various smart cities around the world that use IoT. This type of smart cities is starting to transform all public institutions, changing their culture, from one control-based to one performance-centered. IoT is starting to play an important role in smart cities' evolution and it brings an improvement in the government-citizens relationship. We have identified that although technology is a central element, there should also be considered the capability and willingness of citizens and public institutions to collaborate in order to implement the best solutions for the communities.

1. Introduction

We consider important to firstly mention the research question of this paper, which is the following one: „Is there any missing link between the Internet of Things and the development of smart cities and, if yes, what might that link be?". The information presented in this article will be of aid in finding an answer to this question.

The Internet of Things concept (known in the literature as IoT) is not as new as one might think. It first appeared in 1999 when Kevin Ashton, the British who created the RFID (Radio Frequency Identification) systems standards, used it to describe a system in which the Internet connects to the physical world through sensors [2], these having the role of collecting data for sending them over networks to servers. Since back then he described how the devices connected to the Internet will change our lives, which nowadays is already far from being science-fiction. We see everywhere around us either cars connected to the Internet (via GPS terminals installed on board), industrial or agricultural equipment remotely coordinated through the Internet, drones, even refrigerators and washing machines (the smart mobile phones, present in everyone's pocket, are the best proof of the development of this IT industry's segment).

Today, the total number of connected equipment reached 23.14 billion, with the prospect of reaching 75.44 billion in 2025 [19].

[1] SNSPA, Bucharest, Romania, e-mail: tirziu.andreea@yahoo.com
[2] SNSPA, Bucharest, Romania, e-mail: cataloi@yahoo.com

The main components of an IoT system are the following [22]:

- **Data collection equipment** – some examples here would be: sensors, mobile phones, etc.;
- **Communication networks** with the role of connecting the equipment mentioned above – such as Wi-Fi, 4G, Bluetooth etc.;
- **Servers and other computational systems** that use these data – such as: storage, analysis devices or dedicated software applications.

When all three of these components are found in the same system with the role to deliver services (and sometimes products), then we can really talk about added value created with the aim of developing citizens, the public and the private environment. A short example would be the smart devices that monitor the evolution/involution of a chronic disease in a patient by transmitting real-time data to doctors who may intervene if the situation requires so.

IoT applications and systems are organically developed – based on needs, but the impact they have on us depends on the degree of acceptance of new technologies by citizens, the public and the private sector [23].

The greatest risks that can arise from the extensive use of IoT come from the data security and cyber attacks area. However, the laws of the economy must be understood, namely that the most trustworthy products and services will continue to be procured by the beneficiaries – demand and supply are strongly connected. The Statistic Portal tells us that the IoT market has exceeded a trillion dollar at the end of 2017, forecasting an evolution of up to 1.7 trillion dollar at the end of 2019 [20].

2. Cities with senses

More and more cities in the world are experiencing the new dimension of sensor networks. Many are involved in pilot projects with the purpose of monitoring various activities in urban life, such as the level of noise or air pollution, parking management, health monitoring applications for persons suffering from chronic illnesses etc. **Thingful** is a search engine within this new dimension of the digital world. It contains indexes with the geographical positioning of all the fixed equipment connected in the world – a simple typing of a city's name can indicate on the map where different sensors are placed and what function they fullfil [21].

Thingful's goal is not just to provide a map of existing public or private equipments, but also to provide developers with solutions for smart cities to use these devices – of course, with the consent of the owners [21].

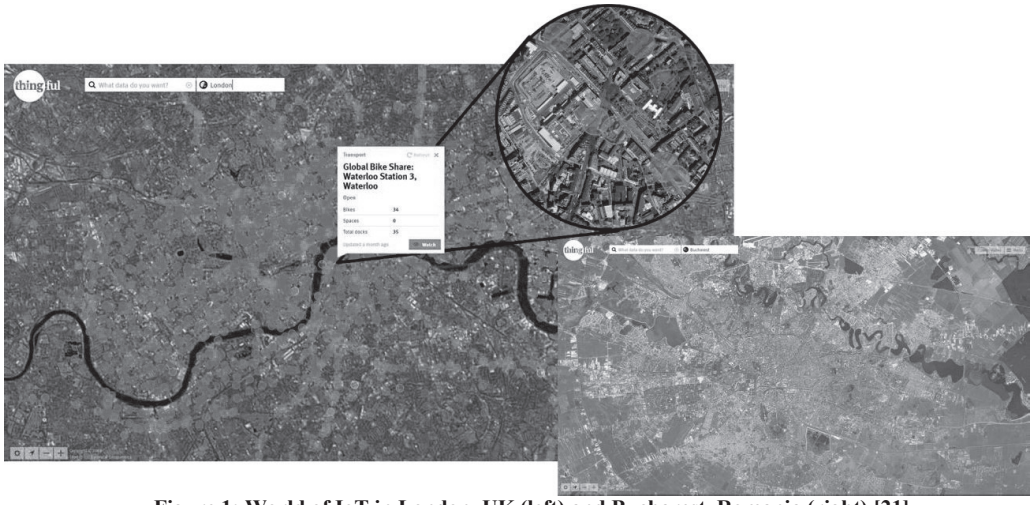

Figure 1: World of IoT in London, UK (left) and Bucharest, Romania (right) [21]

London has developed, with six partners, including Future Cities Catapult and Intel Collaborative Research Institute, the project **Sensing London**. Five living labs were built around the metropolis to collect data (obviously through sensors) about humidity, air quality, traffic and pedestrian activity. Subsequent analyzes directly help enrich the knowledge of how British capital residents use the infrastructure. At the same time, indirectly, these data are used as inputs in the health, environment and life comfort systems due to the statistical analyzes that can be carried out and thus the impact that a particular phenomenon can have in the area of interest researched can be predicted. From this point to developing new solutions (such as an application that would help asthmatic patients to travel through the city) or to developing new business models that allow the expansion of green spaces without major financial investment or even the justification for the development of new technological infrastructures is just one step [11].

The Christchurch city of New Zealand has developed, through a nonprofit organization, a similarly project called **Sensing City Trust**. The actors involved want to better understand how data gathered through sensors can help mayors to develop better public policies. After a devastating earthquake in 2011, a network of digital sensors was developed and installed as part of the city‘s physical infrastructure in order to gather information on air quality. In addition, 150 people registered in the public health system were recruited as chronic respiratory patients who were given a „smartinhaler“ which records where and when they are using medication to relieve symptoms. The data is then automatically transmitted via the smart phones the individuals owns, to a secured database, overlapping those that come from the sensors we mentioned and which were collected shortly before, and thus offered to decision makers for them to be able to develop the most effective public health policies. Supplementary to the initial purpose of the project, the information produced by the analyzes help doctors to improve their understanding of chronic lung diseases, thus managing to bring real benefits to patients by the fact that they can get treatment before reaching the hospital – in the event of an intervention, medical crews already know the condition of the patient, his/her needs and implicitly their response time is being reduced [15].

Chicago, in the United States, has developed a matrix of equipment – **Array of Things**. This is an interactive network of modular sensors that collects real-time data from the environment, from the physical infrastructure of the city, as well as those that target the behavior of citizens. The goal is

obviously to better understand the local urban environment and the impact it has on the lives of individuals living and working there – the most important elements for analyzes being those related to climate, air pollution and noise pollution. The data thus collected are open, meaning that are open to free use by residents, software developers, scientists or decision-makers. Citizens‘ behavior is detected through three different types of sensors: sound sensors, which collect data from the surrounding environment; infrared cameras oriented to car or pedestrian traffic areas and which are designed to record temperatures from the surface of fixed or in motion objects; and a wireless network that measures the number of nearby Bluetooth and Wi-Fi devices – it acts as a proxy for pedestrians in the area. Although questions can be raised that would concern the privacy area of citizens, the project guarantees that no personal or identification data are collected [1].

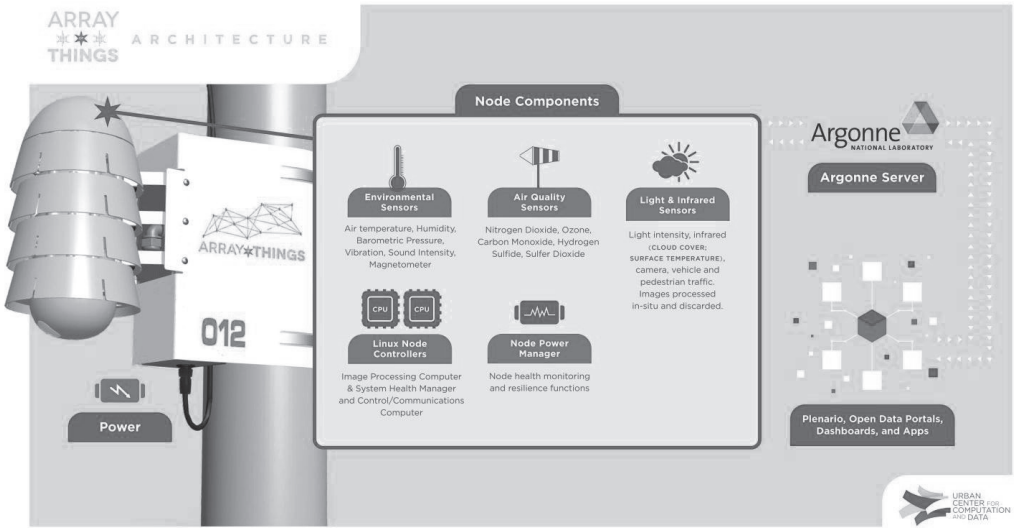

Figure 2: Architecture of the Array of Things system [1]

In Sibiu, Romania, was developed, thanks to the collaboration of „Lucian Blaga“ University of Sibiu with the University College of Southeast Norway, Norway, the project **A Mobile Platform for Environmental Monitoring** with the aim of producing an environmental map that provides all actors in the city‘s perimeter with information on air quality and noise pollution. The Faculty of Engineering within „Lucian Blaga“ University has developed hardware modules that can be placed on cars and which are meant to collect traffic data both when the car is in motion or in the parking areas, when the car is parked. The collected data is transmitted via a GSM module combined with a GPS module implemented on the equipment to a server that has the role of storing them and providing them for analysis to the actors involved. Two prototypes of sensors were realized, the last of them (and the most advanced) being able to collect both data such as the CO_2, NO_x level as well as the amount of suspended solid particles. The project is still in the pilot phase, with only 16 cars equipped with such modules in the city, being completely functional, a number of aproximately 100 units will be produced to be mounted on vehicles [4].

Figure 3: Data collected through mobile traffic platforms in Sibiu [9]

Therefore, we can see that IoT is spread all over the world and these various cities, mentioned above, have successfully implemented this concept and were given as examples in this paper in order to emphasize the ways in which IoT networks and services can contribute to develop smart cities, thus shaping even more the path to proving an answer to our research question, mentioned in the introductory section.

3. Some of the main risks of a connected city

IoT will bring innovations within smart cities, but with the creation of new innovations also arise difficult challenges. Some of the main and most common risks that the implementation of IoT can bring to smart cities are the ones mentioned below.

3.1. Cyber security

As our cities are becoming more and more saturated with sensors, they are becoming smarter and smarter [5]. However, we must also take into account citizens' degree of tolerance for the invasion of data collection equipment – as the number of equipment increases, the citizens feel more supervised [24].

The most common questions here are: (1) „Who produces and controls the equipment?", (2) „What do they measure?", and (3) „Who has access to the data?". All these questions are important and answers to them must be available to every citizen in a language that is as easy to understand as possible so that there is no confusion.

Other questions such as those related to the purpose of collecting data, the changes that will follow from these operations and the benefits of citizens, the public and the private sector are also important. Data storage management mechanisms (often software) are also commonly found in studies about IoT.

Many cities consider elements of security (obviously not only digital) and intimacy as key to sustainable and harmonious development. The level of trust and acceptance of the new by citizens is crucial in developing smart solutions. However, there is little written information on how citizens see these things.

The European Union, being concerned with this topic, has created the GDPR (General Data Protection Regulation) guide, which will start taking effect on May 25, 2018. Formaly known as EU 2016/679, this new regulation replaces Data Protection Directive 95/46/EC and has the aim of unifying the laws on data privacy from EU member states in order to protect and strengthen data privacy of European data issues. It also has the purpose to provide a uniform framework regarding the protection of personal data, thus strengthening the EU digital market [8].

Dan Gârlașu, from Oracle Romania, warned IT users that in the future smart cities may be more vulnerable to hackers than smart computers and smartphones are today [12].

With billions of interconnected devices all over the world, cyber security challenges are increasingly addressing also the IoT dimension of the digital world. Often the media poses on the front page of the newspapers titles that refer to hacking actions of different types of equipment. In the summer of 2015, the car producer Fiat recalled 1.4 million vehicles for software updates due to the risks of the machine safety being affected [3]. At the end of 2017, a clip posted on Youtube featured two hackers who stole a luxurious car by remotely cloning the door opening device and starting the vehicle [25]. Shortly after the event, CNN tech has produced the „Watch thieves steal car by hacking keyless tech" material explaining each action of the hackers [6].

Cesar Cerrudo, Chief Technology Officer of IOActive – one of the most prestigious digital security consultancy corporations, stated for The Independent in the UK that „a malicious hacker could use the information to manipulate traffic lights to cause jams and alter speed limits" [18].

***

This research area is particularly rich in topics. The European Union Agency for Network and Information Security (ENISA) launched in November 2017 some recommendations on IoT security in the context of critical information infrastructures [7]. Microsoft, Symantec, along with other leading companies in the cyber field regularly make reports on case studies accompanied by warnings and recommendations on this new dimension of the digital world: „Developing a City Strategy for Cyber Security" [14], „Transformational 'Smart Cities': Cyber Security and Resilience" [16]. Unfortunately, however, there is little information on how these recommendations are embedded in smart solutions implemented at city level.

Cyber security efforts tend to be focused on the role of local leaders in the development of smart cities and the IT&C embedded systems, although it is known that the development of such cities is much more complex, involving many partners in this process and as many technologies.

3.2. Temporary inoperability

IoT enthusiasm is often tempered by the connectivity problems that the equipment are faced with. The wireless ecosystem, though easy to understand, is hard to imagine. Due to the very large number of IoT uses, we cannot find a single standard – both in wireless technologies and in electricity consumption [17]. These two seemingly minor problems can cause major effects in the good functioning of an IoT system.

The technology of a smart city could be taken by surprise by the technological advances – new equipment is being developed, with new standards long before the old and already in motion ones are depreciated. Hence, many connectivity problems can arise between the equipment placed in the

wireless ecosystem of IoT. For example, we can imagine a smart city in which automated cars (without a driver) navigate by themselves on the city's streets. What happens when they pass through an area in which the sensors of the traffic lights are no longer compatible with theirs? Another question that arises is what happens when, due to network noise, communication between the vehicle and the traffic light system is slow or temporarily interrupted? Obviously, these questions must first find an unequivocal answer in order to be able to talk about a successful implementation of such a system [13]. In Figure 4 we can see the complexity of such a system and, practically, due to the large number of devices that need to communicate in a very short time, the risks associated to a small data flow disruption.

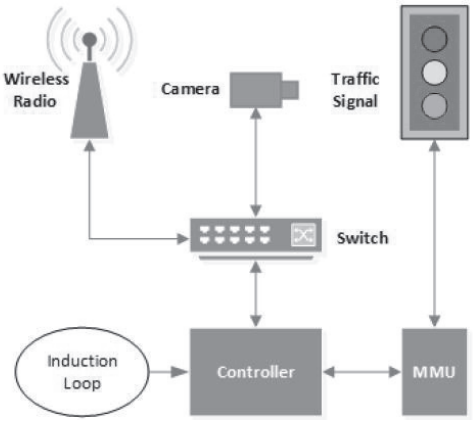

Figure 4: A typical traffic intersection [13]

All Internet users experienced situations where web pages were loading slower or when mobile calls were disrupted apparently for no reason. These situations can create frustration, but humans understand and know they can appear. But when we talk about electronic equipment, they cannot understand, and the effects of their misunderstanding can produce less pleasant effects for citizens or the environment.

If, in the case of the cyber security risks previously presented, the pressure was on the managers of a smart city, in the case of interoperability, the pressure tends to be put on the research environment, especially in the technological and academic areas. Only these can find viable solutions to such problems.

4. Conclusions

The dimension of IoT is not just a goal to be achieved – often mayors, hearing the concept but not understanding it in its depth, want to invest in IoT sensors and equipment for their cities – it is a remarkable symbiosis between society and technology. Many of those technologies that once represented the top ones are today viewed as part of everyone's life.

The parallel between IT and Internet innovations has led to a series of changes in the world economy such as the growth of the sector of products and services dedicated to informational economy. As Thomas Lauren Friedman (a New York Times journalist) said in his book „The world is flat: A brief history of the twenty-first century", written in 2005, „the Internet has flattened the

world, IT has first provoked and then increased the pace with which these changes have occurred, providing a platform for development" [10].

Of all the challenges of the electronic world, IoT is the newest and probably the biggest – due to the explosive evolution of the number of Internet-connected equipment. It must be well known, understood and managed. There is a hidden component in people's Internet, also known as Deep Web or Dark Web, where unknown operations are made and of which only the actors directly involved have a clue. Many of these operations are illegal. Why wouldn't the Internet of Things risk to have its own dark side? To minimize this risk, a proper education of all stakeholders is required, so that the responsibility for a successful system management will be implicit.

Taking all this information into account, we can observe that the response to this paper's research question is education regarding the concepts mentioned, which will be constituted as a solution to the problems that might occur in the implementation of IoT networks and services in order to contribute to the development of smart cities. Education can increase the capability and willingness of citizens, institutions of the public sector and also private companies to collaborate for implementing the best solutions for the communities. This is thus a subject to be developed in further research.

5. References

[1] ARRAY OF THINGS, https://arrayofthings.github.io/, accessed on 10.12.2017.

[2] ASTHON, K., That ‚Internet of Things' Thing, RFID Journal, http://www.rfidjournal.com/articles/view?4986, accessed on 10.12.2017 (2009).

[3] BBC NEWS, https://www.bbc.com/news/technology-33650491, accessed on 10.12.2017.

[4] BERNTZEN, L., JOHANNESSEN, M.R., FLOREA, A., Smart Cities: Challenges and a Sensor-based Solution, A research design for sensor-based smart city projects, International Journal on Advances in Intelligent Systems, http://www.iariajournals.org/intelligent_systems, Publisher: International Academy, Research and Industry Association (IARIA), volume 9, issue 3 & 4 (2016).

[5] BUSINESS INSIDER, How smart cities & IoT will change our communities, http://www.businessinsider.com/internet-of-things-smart-cities-2016-10, accessed on 10.12.2017 (2016).

[6] CNN TECH, Watch thieves steal car by hacking keyless tech, http://money.cnn.com/video/technology/2017/11/28/relay-box-car-theft.cnnmoney/index.html, accessed on 10.12.2017 (2017).

[7] ENISA, Baseline Security Recommendations for IoT, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot, accessed on 10.12.2017 (2017).

[8] EUGDPR, https://www.eugdpr.org/, accessed on 05.03.2018.

[9] FLOREA, A., BERTNTZEN, L., Green IT solutions for smart city sustainability, paper presented at the Smart Cities Conference, 5th edition, December 8, 2017, SNSPA, Bucharest, Romania (2017).

[10] FRIEDMAN, T.L., The World Is Flat: A Brief History of the Twenty-First Century, Farrar, Straus and Giroux, New York (2005).

[11] FUTURE CITIES CATAPULT, Sensing London, http://futurecities.catapult.org.uk/project/sensing-london/, accessed on 10.12.2017.

[12] GĂRLAŞU, D., Cyber Security Update on Threats and Trends, paper presented at the Smart Cities Conference, 4th edition, December 2016, SNSPA, Bucharest, Romania http://administratiepublica.eu/smartcitiesconference/2016/program.htm (2016).

[13] GHENA, B., BEYER, W., HILLAKER, A., PEVARNEK, J. and HALDERMAN, J. A., Green Lights Forever: Analyzing the Security of Traffic Infrastructure, Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT '14), August 2014 (2014).

[14] MICROSOFT CORPORATION, Developing a City Strategy for Cyber Security. A seven-step guide for local governments (2014).

[15] SENSING CITY, http://sensingcity.org/, accessed on 10.11.2017.

[16] SYMANTEC OFFICIAL BLOG, Transformational 'Smart Cities': Cyber Security and Resilience, https://www.symantec.com/connect/blogs/transformational-smart-cities-cyber-security-and-resilience, accessed on 10.11.2017 (2013).

[17] TEXAS INSTRUMENTS, Wireless connectivity for the, Internet of Things: One size does not fit all (2017).

[18] THE INDEPENDENT, Vulnerabilities in traffic light sensors could lead to crashes, researcher claims, http://www.independent.co.uk/life-style/gadgets-and-tech/news/traffic-light-hack-could-lead-to-road-chaos-claims-expert-9309936.html, accessed on 10.12.2017 (2014).

[19] THE STATISTIC PORTAL, Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, accessed on 05.03.2018 (2018).

[20] THE STATISTIC PORTAL, Size of the global Internet of Things (IoT) market from 2009 to 2019 (in billion U.S. dollars), https://www.statista.com/statistics/485136/global-internet-of-things-market-size/, accessed on 10.12.2017 (2017).

[21] THINGFUL, http://www.thingful.net/, accessed on 10.12.2017.

[22] UK RS ONLINE, https://uk.rs-online.com/web/generalDisplay.html?id=i/iot-internet-of-things, accessed on 10.11.2017.

[23] VRABIE, C., Elements of E-Government, Pro Universitaria Publishing House, Bucharest (2016).

[24] VRABIE, C., Your freedom starts where my privacy ends, Smart cities, Pro Universitaria Publishing House, Bucharest (2017).

[25] YouTube, https://www.youtube.com/watch?v=bR8RrmEizVg, accessed on 11.12.2017.

RESEARCHERS AS MEDIATORS BETWEEN POLICYMAKERS AND PRACTITIONERS – DO THEY HAVE THE NECESSARY SKILLS?

Adriana Zaiţ[1]

DOI: 10.24989/ocg.v331.23

Abstract

Scientific research is nowadays a larger endeavor than ever, and researchers more than ever overwhelmed by questions of purpose, trust and future prospects, seen as either saviors and providers of solutions, or cash generating machines through altered and irreproducible results. Research is conducted in various social structures contexts, which shape everything from the questions asked within a society to the way responses given by researchers are used by policymakers and companies. It is no surprise, in these conditions, that they are often in the middle between policymakers as providers of regulations and funding, and practitioners as providers of markets for the products and ideas obtained through scientific research. Skills required for such a mediation process, for the complex array of informative interactions among various groups of stakeholders and interests are huge, way beyond technical knowledge and abilities in their field of specialization. But are they prepared for this role, as long as educating researchers doesn't necessarily go farther than providing them the methodological background for doing research? Scientific rigor and managerial relevance, communication and education have very different facets for policymakers and for practitioners, and researchers often lack the skills for this ambiguous game of instrumental, conceptual and strategic knowledge development and utilization. The aim of the present study is to analyze the skills inventory necessary for the modern researcher, as perceived by junior researchers, and the way ICTs, eDemocracy and civic participation could help shaping the researcher as mediator between politicians and practitioners. Literature review, in-depth interviews with junior researchers and content analysis are used from a methodological point of view.

1. Introduction – context and objectives

Societies all over the world are more and more confronted with the rapid evolution of various positive advancements and also intricate crises (financial, economic, social, moral, political, health, education, democracy etc.) Various stakeholders are looking for or expecting solutions. Governments and research institutions are among those struggling for finding and applying solutions, and a large civic participation provides the healthy environment for these endeavors. The role of researchers becomes significant in ensuring a long-term success, including for the modern forms of e-Societies – e-Democracy and e-Governance. From all stakeholder categories (i.e. citizens, service users, businesses, public administrators, government agencies, not for profit entities, politicians, educators), researchers are the most complex one, with multiple facets and multiple roles: they are specialists in their fields, citizens and constituents of the public opinion, members of funding agencies and administrative entities, sources of information and educators,

[1] University "Alexandru Ioan Cuza" Iaşî, Romania

influencers and beneficiary of research results, at the same time. But are they prepared to perform all these roles, do they have the necessary abilities for being such a complex actor and interface, at the same time? This is the main question of the present study, an exploratory one, meant to clarify the mediating position of researchers in the present, post-modern society. The main objectives are to synthesize the roles and skills for modern researchers, according to the literature, and identify the perceptions of researchers toward their mission in the present society.

2. Skills for research and a search for new skills – a literature review

A thorough literature review was performed, at the intersection of three fields – research (theoretical and applied, academic and business research, researchers skills and abilities, research results' use and dissemination etc.), public policies and strategies (policymakers, politicians, governments, decisions etc.) and e-governance (social media role, e-democracy, e-government stakeholders etc.). This documentary study allowed us to obtain a detailed view of researchers roles and correspondent skills, as emphasized in previous studies.

There are very few comparative analyses of the roles and perspectives of various categories of stakeholders, as previous studies discovered, as well (Yildiz, 2007; Rowley, 2011), and almost none considering researchers as a separate important stakeholder category. Yildiz considers that a better explanation of stakeholders' participation requires an enhanced understanding of the e-government process, which has a definitional vagueness at this time, so more research should be done in the field. Rowley's study is the only one found in which the typology of e-government stakeholders roles includes researchers and evaluators as a separate category (12 categories are identified – people as service users, people as citizens, businesses, small-to-medium sized enterprises, public administrators, other government agencies, non-profit organizations, politicians, e-government project managers, design and IT developers, suppliers and partners, researchers and evaluators). Only two other studies mention research institutions (Heeks, 2003) and researchers (Millard, 2008) among various interest groups and roles. Overlaps and conflicts may also be present when talking about researchers' roles and interests, with several distinct value dimensions – technical (own specialty), financial, social, political, personal (identity and career). The societal values, as a whole, have changed in time, from liberal ones during the 18th century, through democratic values (19th) and social values (20th), to empowerment values in 21th century (Millard, 2010), and researchers values and roles changed or should change accordingly; researchers cannot limit anymore to their technical-innovative, specialized and somehow isolated role of discoverers, they need to be active participants to the civic life of their communities.

One important barrier for researchers' increased participation and mediating role relates to the different professional cultures of various stakeholders categories (Ginsburg & Gorostiaga, 2001; Anderson, Herriot & Hodgkinson, 2011; Hanover Research, 2014; Rex, 2015). If we are looking just at researchers and economic environment representatives we can see that the first category highly values scientific rigor, while the second category places a great weight on practical relevance; irrelevant theory and invalid practice could lead to inefficient fragmentation of efforts and a lack of sense in research. As Anderson, Herriot & Hodgkinson (2011) found, a 2 x 2 model of research or science exists, in terms of high and low levels of relevance and rigor, in which we can talk about four major types of science – pedantic (high rigor, low relevance), pragmatic (high rigor, high relevance), popularist (low rigor, high relevance) and puerile (low rigor, low relevance). Academic researchers tend to be pedantic, organizational clients and companies tend to be popularist, and from their contradictory struggle science is rather loosing, becoming puerile. In order to move to the pragmatic level, researchers should engage more in civic and especially

political activities, in order to equilibrate expectations and influences of various stakeholders and to find a common language, rigorously correct, yet easy to understand by non-specialists in the field. The measures of success for researchers' outputs need to move from selfish ones, in which the researcher is the main beneficiary (publications, evaluation indexes, promotion etc.), to service-oriented ones, in which the accent is on others - economic, social, cultural etc. - benefits (Kern, 2011).

In order for such a change to take place, researchers' "normal", usual skills, related to methodological rigor, specialized knowledge in the field, analytic accuracy, scientific enthusiasm, resilience etc. are not enough. Political skill, defined as an ability to effectively understand others at work and use knowledge to influence others to act in ways that enhance one's personal and/or organizational objectives (Ferris et al, 2005; Ferris et all, 2007; Treadway et al, 2010; Blickle et al, 2011; Grieve & Mahar, 2013), becomes a "must have". This complex political skill has cognitive, affective and behavioral manifestations, influencing both directly and indirectly the outcomes of research, as it was long time ago hypothesized (Pfeffer 1981, Mintzberg 1983), and as recent studies have shown (Treadway et al, 2010; Braddy & Campbell, 2014; Langer & Stewart, 2016; Wise, 2016).

Academic research is crucial for the process of informing government policy (Rex, 2015), and researchers should take up more advisory roles, engage as much as possible with policy makers. Rex metaphorically speaks about researchers as providers of "a ladder out of the ivory tower". If they want to make a difference, researchers need to learn political skills, the art of drawing the correct lines between allowed, banned and controlled approaches, so that they could enable societies to develop (Alexander, 2016). The basic political skills would allow researchers to make their findings accessible to both politicians, who have the power as decision makers, and to the public, as final and real beneficiary. Impact becomes a driver (Smith, 2012), as scientists might have the freedom to decide what research to support, from a scientific point of view, but the research councils, often with political involvement, are those that sets strategic goals in order to contribute to economic growth and social development.

As Wise (2016) noticed, skills are at the heart of productivity and growth, at both personal, collective and social level, but they are also regionally sensitive, suggesting that some sort of skills ecosystems are needed in order to obtain the best impact – and political skills are definitely regionally defined and culturally affected and should be considered in such an ecosystem. They are strongly related to a larger category of skills, labeled as social intelligence (Grieve & Mahar, 2013), which includes social skills, social information processing, social awareness and also connects with emotional intelligence and empathy. Four distinct practices are usually associated with political skill as general ability to maximize and leverage relationships in order to achieve individual, team and organizational goals (Ferris et al, 2005; Braddy & Campbel, 2014): social awareness or astuteness (as the ability to observe others and understand their behaviors and motives); interpersonal influence (as a person's ability to influence and engage others, in a compelling and charismatic style); networking (ability to build relationships across and outside the organization); sincerity (ability to be forth right, open, honest and genuine with other people). This is the type of skill one would also expect to find in the category of transversal and transferable skills (Bimrose et all, 2007), highly valued, on theory, yet les often really developed at academic level, unfortunately.

When they disseminate their research results, researchers usually target other researchers, publishers and financing bodies but, as Langer & Stewart (2016) stated, "piles of evidence don't make any difference if they're not used to develop policy". This suggests that researchers should

tailor and address their communication of research findings to policy makers, as well, especially considering various orientations and parties, because policymakers of different political colors can act as bridges between groups and departments, increasing the interdisciplinary and applied focus. This approach is not an easy one and it is not risk free, there is a long history of concern with the impact of research on policy (Ginsburg & Gorostiaga, 2001). It is almost common practice that vital decisions in a country are often taken without sufficient information or sound knowledge, sometimes from ignorance, sometimes due to honest limits, and sometimes deliberately, for political reasons. Ginsburg and Gorostiaga (2001) speak about three large types or categories of knowledge utilization, two positive and one negative. The positive ones are instrumental and conceptual use, and the negative one is dangerously labeled strategic, although it is considered a knowledge misuse. In the instrumental approach knowledge from research is used directly in making specific decisions, in processes which are of knowledge driven type (basic or theoretical, fundamental research, followed by applied research, development and application in economy and society) or problem solving type (a policy problem is identified, research is performed and a solution is suggested). The conceptual type is more complex and diffuse, rather indirect, and consists of two sub-categories of knowledge use, interactive and enlightenment type. In the interactive approach research findings are used by policymakers together with their own political experience and along with opinions from various other economic and social actors, in a non-linear, complex process of decision. In the enlightenment type of approach, scientific concepts and research results are spread in the whole society, through some type of diffusion process, thus shaping the decision makers' general way of thinking and becoming relevant to policy; it is a sort of educational process taking place in society, but the mechanisms are neither unique, nor simple to explain. The third type of use of research knowledge, the negative one, has three sub-categories – political, tactical and promotional. In the political type of use, research findings are considered and applied selectively, to support a previously adopted political decision – only results supporting a specific position are actually taken into consideration, contrary ones being ignored. In the tactical type, research is used to enhance the credibility of policymakers and actions or – quite often – lack of action. Research results are rather excuses or status building accessories among politicians. Finally, in the promotional type research serves to disseminate and promote the implementation of a specific policy to individuals and groups who were not involved in the decision-making process. These types of uses can take place continuously, all the time, but can also prevail in specific stages of the political process, as Klemperer, Theisens & Kaiser (2001) suggest. In their view, not always supported by empirical facts, the conceptual enlightenment occurs more often in the design stage of policies, the strategic political one during the decision stage and the instrumental problem solving one during the implementation stage. Various supplementary problems arise, due to the different cultural backgrounds of researchers and policymakers, researchers being usually seen as more objective, in favor of factual knowledge and dispassionate, universal truth, while policymakers are usually perceived as subjective, partial, biased, incomplete, focusing on self-serving and politically compromised knowledge. However, solutions exist for the mediation of this complex process between researchers and policymakers, six approaches being suggested toward enhancing the connections and collaboration among theorists, researchers, practitioners and policymakers: translation, education, role expansion, decision oriented research, collaborative action research and collective research and praxis. For the first translation approach, researchers are mediators, labeled as research brokers or linkers, supposed to find a common language for all stakeholders. The education approach goes a bit further, for both researchers and policymakers, but it remains a question of superficial transformations, at the surface – focus on communication and negotiation, rather than common work. Role expansion suggests the involvement of every category in the activities of the others – practitioner research, policy assisting roles for researchers – it is the start of actually being in the other category's shoes. The last two forms, the most evolved ones, require

more and more joint reflexion and action, co-learning and real collaboration for a common societal aim. No matter what the adopted solution is – simple translation or real collaborative work - the first step is to prepare researchers to the political skill type of abilities necessary to generate the positive change, otherwise the process cannot be initiated. But do we prepare researchers for such a job? The answer is rather no, at this moment – political skill doesn't appear in academic curricula or research institutions job descriptions, all over the world, and both academia and research entities are rather reluctant to engage in policymaking consulting or joint activities.

3. Researchers as mediators – methodology and results

In order to find out what researchers think about supplementary skills in the e-society, without any hint about the purpose of the study, not to influence their opinions in any way, we performed a loosely structured exploratory study. The exploratory study consisted of a semi-structured qualitative survey with 12 junior doctoral researchers. They all received 5 open questions, for which the answers were provided individually, in a written format; the whole process took one hour, every researcher taking as much time as needed in order to reflect and answer. The questions were: (1) What is the main role or mission of a researcher nowadays, in the present society? (2) Apart from the specific research skills, what other abilities would be useful for a researcher? (3) Who could and should use the research results, and how could this be done? (4) How do social media and eGovernance influence the position and mission of researchers? (5) Thinking of your overall research experience, please tell which is the most representative story/happening/memory you could share? We selected the first four questions in relation with the main issues identified in the literature review (researchers' roles in society, skills for researchers, use of research results, research and e-governance) and our main research question (do researchers have the skills required to accomplish their complex role in the e-society). The last question was a story telling type, designed for indirectly and most credibly obtaining information about the most important issues in the research activity of the interviewed researchers. Questions were addressed one by one, in a logical sequence, with time for answering in between, so that respondents would not be influenced by the final aim. The data collection method is a mixture of interviewing, qualitative survey and group interview, with certain advantages in terms of time and ease of collecting.

Answers were analyzed using an emergent coding content analysis procedure, with no pre-established categories, due to the exploratory intent of the research. Written texts were read three times – first time for getting a general idea or image, second time for identifying main categories (presence of specific issues of interest) and the third time in order to evaluate weight (most frequent issues for every researcher and for the whole group of 12) and affect (positive-negative, optimistic-pessimistic). We will present the finding in the next paragraphs.

For the first question, concerning the perceived mission of the researchers, 6 answers were uni-dimensional – one single important mission, 5 bi-dimensional – two related missions and one tri-dimensional. As single important mission (present in all 12 answers) it was seen the contribution to the positive evolution of the society, with small variations (development of science for a better life, providing solutions for the society, bringing benefits to the society, finding relevant answers for the population, offering explanations for the changes in the modern society). A second mission (present in 5 answers) was related to finding causal explanations, influencing human behavior, becoming a binder between economic, academic and legal environment, bringing novelty or obtaining innovation (not necessarily connected to practical solutions to be applied in society). The third mission was related to the ability of making predictions, knowing what the future will bring. Although all missions are interconnected, the practical side of the research was emphasized – the

positive development of society – but at a very general level, without specific issues being discussed.

For the second question the junior researchers provided a list of supplementary skills related to the ”soft” abilities – communication (mentioned 5 times), perseverance (mentioned 3 times), passion (mentioned twice), attention to details (mentioned twice), courage, patience, confidence, open-mindedness, flexibility, socialization, team working, human interaction, entrepreneurial spirit, empathy, time management, desire to learn, cultural sensitivity.

The third question – a double one – had precise answers only for the first part – who could/should use the research results. In terms of how, only three answers were given – when decisions are taken, when it's a need and through the creation of an appropriate framework - again, very vague, general answers. As for users, four categories of stakeholders were - mentioned: government and state institutions (9 answers), business environment and companies (6 answers), academic and research entities (5 answers), civic society (3 answers).

For the fourth question there were two aspects investigated – the presence of specific influences and the direction of those influences, positive or negative. Only three researchers gave negative interpretations for the social-media effects – too many information and too little time for analysis, lack of credibility, manipulations possible, and errors of interpretation. Two of them only gave negative effects, one talked about both positive and negative influences at the same time. As for the positive influences, they were mainly related to easy and rapid access to information, for both documenting and disseminating results (10 answers). One answer concerned the positive pressure of social media channels on entities which are supposed to use the research results (talking about social media as a new power in a state), one about the smaller distance between researchers and consumers of research results, talking about a researcher's stepping down from the pedestal, out of the usual “bubble”, and one about the shorter time between discovery and application of research results, through convincing political decisional factors about the opportunity of research results implementation.

The story telling was least successful, due to the written form, most probably, but also to the limited experience of the junior researchers. Stories were very short, not elaborated. 3 of the researchers said only that they would talk about a specific issue (finding out others' opinions for their research, explaining an intended model of research and what is the position of the researcher), without providing the real story (they only said they would tell this story). The other stories shown the importance placed by researchers on the recognition of their efforts and results (the fact that they received appreciation from the coordinator, they succeeded to go to a conference or publish an article, they were able to find other people doing similar things and appreciating their work) or the difficulties encountered in their research endeavors (lack of data, lack of cooperation from the part of the investigated companies, fear that the results would not be those expected, desire to give up, fear that everything was already researched and said and nothing new could be discovered).

On total the researchers seem to be aware of the fact that they have a special role to play for the advancement of the society, but without offering precise details about this role. They did not emphasize other potential roles, either – users of research results, influencers or consultants, for example. They have a rather passive position as far as the use of the research findings is concerned – a perspective in which their research results should be used by state institutions, companies and the academic environment, mainly, without a particular initiative from their part. It looks like their mission is rather to do research, and then somebody else should actually use the results in order to

produce the positive evolution in society. The social media is seen as very important, but again more as an information and communication channel. As for skills, most of the answers focused on general communication and other soft skills related to research – attention to details, courage, curiosity, openness, perseverance. There were no answers related to social astuteness, interpersonal influence, networking and sincerity, as potential dimensions of the political skill inventory. The story telling didn't bring anything new concerning situations in which the political skills would be needed, meaning that at an exploratory stage, with a totally open discussion, junior researchers don't seem to be aware of a need for political skill.

4. Conclusions

The specialized literature shyly writes about researchers as distinct and important stakeholders in the modern society or about their complex, multiple role. The impact of research on practice and policy is questioned and worrying, yet specific approaches and instruments for improving this impact are not developed. The way policymakers use research results is not always positive, and the professional culture differences between researchers and policymakers are large, recognized but still not treated. However, studies already draw attention on the potentially significantly positive consequences of the real collaborative approaches between researchers, practitioners and policymakers. Special political skills are needed for this collaborative process, and even if the subject is rather old, starting back in the 80's, it's only lately that investigators conceptually defined and conceived operational measures for the new type of abilities (2005, through the Ferris et all approach of defining and measuring the political skill construct).

An exploratory study on 12 junior academic researchers (PhD level, from the field of economics and business administration, sub-fields accounting, computer science, economics, international relations, finance, management, marketing, statistics) has shown that researchers are aware of their special role in the advancement of the society and making life better, but without seeing the precise details of this role or how it could be performed. They did not emphasize other potential roles, as for example users of research results, influencers or consultants, roles suggested by Rowles (2011). They have a rather passive position toward the use of their research findings; their research results should be used by state institutions, companies and the academic environment, mainly, but apparently without any particular initiative from their part, they don't seem to acknowledge their contribution in initiating such a process. It looks like their mission is rather to just do research, and then somebody else should actually use the results in order to produce the positive evolution in society. The social media is seen as very important as an information and communication channel, and less for a real participation to the e-governance process. As for supplementary skills needed by researchers, most of the answers focused on general communication and other soft skills connected with research – attention to details, courage, curiosity, openness, perseverance. There were no answers related to social astuteness, interpersonal influence, networking and sincerity, as potential dimensions of the political skill inventory. The story telling didn't bring anything new concerning situations in which the political skills would be needed, meaning that at an exploratory stage, with a totally open discussion, junior researchers don't seem to be aware of a need for political skill.

Certain limits exist for the present study – the scarce literature in the field, the delicate subject of the relationship between research and policymaking, the small sample for the exploratory study. However the results are encouraging for future research, extended on senior researchers from research entities, having a permanent research job, and on policymakers, to catch the other side of the equation. The present results should serve as a reflective signal for the academic environment,

concerning the need for developing political skills for future researchers, if we want research results to have a real, positive impact in society.

5. References

[1] ALEXANDER, T. (2017), *Practical Politics: Lessons in Power and Democracy,* Trentham Books, Kindle Edition.

[2] ANDERSON, N., HERRIOT, P., HODGKINSON, G. P (2001), "The practitioner-researcher divide in Industrial, Work and Organizational (IWO) Psychology: where are we know and where do we go from here?", *Journal of Occupational and Organizational Psychology, 74, pp.391-411.*

[3] IMROSE, J., BARNES, S-A, BROWN, A., HASLUCK, C., BEHLE H. (2007), "Skills diagnostic and screaning tools: a literature review", *Research Report n.459,* Department for Work and Pensions, under licence from the Controller of Her Majesty's Stationery Office by Corporate Document Services, Leeds, St Clements House, 2-16 Colegate, Norwich NR3 1BQ.

[4] BLICKLE, G. et al (2011), "Fit of the political skill to the work context: a two study investigation", *Applied Psychology: an International Review,* pp.1-28.

[5] BRADDY, Ph., CAMPBELL, M. (2014), "Using Political Skill to Maximize and Leverage Work Relationships", *White Paper, Center for Creative Leadership.*

[6] CHAMORRO- PREMUZIC, T., ARTECHE, A., BREMNER, A.J., GREVEN C., FURNHAM, A. (2010), "Soft skills in higher education: importance and improvement ratings as a function of individual differences and academic performance", *Educational Psychology,* Vol. 30 , Iss. 2, p.221-241.

[7] COOLE, D. (2007), "Expansion and validation of the Political Skill Inventory (PSI): An examination of the link between charisma, political skill, and performance", *Graduate Theses and Dissertations,* http://scholarcommons.usf.edu/etd/680.

[8] FERRIS, G. et al (2007), "Political skill in organizations", *Journal of Management, 33(3),* pp.290-320.

[9] FERRIS, G. et al. (2005), "Development and Validation of the Political Skill Inventory," *Journal of Management*, Vol. 31 No. 1, February 2005 126-152.

[10] GINSBURG, M., GOROSTIAGA, J. (2001), "Relationships between Theorists/Researchers and Policy Makers/Practitioners: Rethinkingthe Two- Cultures Thesis and the Possibility of Dialogue", *Comparative Education Review*, Vol. 45, No. 2, Special Issue on the RelationshipsBetween Theorists/Researchers and Policy Makers/Practioners (May 2001), pp. 173-196.

[11] GRIEVE, R., MAHAR, D. (2013), "Can social intelligence be measured? Psychometric properties of the Tromsø Social Intelligence Scale – English Version, *The Irish Journal of Psychology*, 34:1, 1-12, DOI: 10.1080/03033910.2012.737758.

[12] Hanover Research (2014), "Buiding a culture of research: recommended practice", *Academy Administration Practice* report, p.1-33.

[13] HEEKS, R. (2003), "Most e-government-for-development projects fail; how can the risk be reduced?", *IDPM*, http://idpm.man.ac.uk/publications/wp/igov/index.shtml.

[14] HODGKINSON, G. P., HEALEY, M. P. (2008), "Toward a (Pragmatic) Science of Strategic Intervention: Design Propositions for Scenario Planning+, *Organization Studies*, 29(03): 435–457.

[15] KERN, S. (2011), "Analytic model for academic research productivity having factors, interactions and implications", *Cancer biology & therapy,* 12, pp.949-956.

[16] KLEMPERER, A. M., THEISENS, H. C., KAISER, F. (2001), "Dancing in the dark: the relationship between policy research and policy making in Dutch Higher Education", *Comparative Education Review*, vol.45, iss.2, pp. 197-219.

[17] LANGER, R., STEWART, R. (2016), "The science of using rsearch: why it starts with the policymaker", *The Conversation,* http://theconversation.com/the-science-of-using-research-why-it-starts-with-the-policymaker-59265.

[18] MEDAGLIA, R., ZHENG, L. (2017), "Mapping government social media research and moving it forward: A framework and a research agenda", *Government Information Quarterly* 34, 496–510.

[19] MILLARD, J. (2010), "Government 1.5 – is the bottle half full or half empty?", *European Journal of ePractice,* nr.9, www.epracticejournal.eu .

[20] MILLARD, J. (2008), "EGovernment measurement for policy makers", *European Journal of ePractice*, nr.4, www.epracticejournal.eu.

[21] MINTZBERG, H. (1983), *Power in and around organizations,* Englewood Cliffs, NJ: Prentice- Hall.

[22] NYGAARD, L. P. (2017), "Publishing and perishing: an academic literacies framework for investigating research productivity", *Studies in Higher Education*, 42:3, 519-532, DOI:10.1080/03075079.2015.1058351.

[23] PANDA, A., GUPTA R. (2014), "Making academic research more relevant: a few suggestions", *IIMB Management Review 26, 156-169.*

[24] PFEFFER, J. (1981), *Power in organizations***,** Boston: Pitman.

[25] REX, H. (2015), "How does academic research contribute to the work of government? - Networks of evidence and expertise for public policy", http://www.csap. cam. ac.uk/news/article-how-does-academic-research-contribute-work-governm/.

[26] ROWLEY, J. (2011), "e-Government stakeholders—Who are they and what do they want?", *International Journal of Information Management* 31 (2011) 53–62.

[27] SMITH, A. (2012), "Making an impact: when science and politics collide", *The Guardian,* https://www.theguardian.com/science/2012/jun/01/making-impact-scientists.

[28] TREADWAY, D. C., BRELAND, J.W., WILLIAMS, L.M., CHO, J., YANG, J., FERRIS, G.R. (2011), "Social Influence And Interpersonal Power In Organizations: Roles Of Performance And Political Skill In Two Studies, *Political Skill, Performance, And Power, p.1-48.*

[29] WISE, G. (2016), "Deceloping productive places: the role of universities in skills ecosystems", *University Alliance Regional Leadership series,* pp.1-28.

[30]. YILDIZ, M. (2007), "E-government research: reviewing the literature, limitations and ways forward", *Government Information Quarterly* 24 (2007) 646–66*5.*

Cybersecurity I

CYBERSECURITY AUTHORITIES AND RELATED POLICIES IN THE EU AND HUNGARY

Tamás Szádeczky[1]

DOI: 10.24989/ocg.v331.24

Abstract
Parallel with the evolving of cyber conflicts, the need for appropriate handling of the public administration tasks also appeared. Governmental tasks were necessary, which includes defense (military), diplomatic, law enforcement and public administrative factors also.

This paper shows an analysis of the institutional background of cybersecurity administration in the European Union and Hungary in parallel. This includes the regulations about ENISA, the European Union Cybersecurity Agency, the Hungarian cybersecurity authorities, and the cybersecurity strategies for both entities, namely Regulation (EC) No 460/2004, Cybersecurity Strategy of the European Union of 2017, Regulation (EU) 526/2013, COM/2016/0410 final, 2017/0225 (COD) Proposal, Hungarian Government decree no. 223/2009, Government Decision no. 1139/2013, Act L of 2013, and Government Decree 187/2015.

The research has been supported by the ÚNKP-17-4-III-NKE-26 New National Excellence Program of the Ministry of Human Capacities.

Keywords: *cyber strategy; information security legislation; incident response*

1. Introduction

The word cybersecurity seems to be a bit overused nowadays, but as other researchers already shown, it is different from the "classical" term information security. In both terms, information-based assets stored or transmitted using information and communication technologies (ICT) is included. But information security also includes paper-based information. The term cybersecurity includes non-information based assets (e.g., a high-voltage substation) that are vulnerable to threats via ICT. This is similar to the interdependency between critical infrastructure elements).[2] The new model of cybersecurity needs a different approach to security organization: the classical security models have to be revised.[3]

The importance of cybersecurity is well-known and often communicated by decision makers. However, the implementation, preparedness, and knowledge have deficiencies. This might happen because of lack of knowledge, resources or experience.

[1] Ph.D., senior lecturer, National University of Public Service, Faculty of Science of Public Governance and Administration, Institute of E-Government, 1083 Budapest, Üllői út 82., Hungary, szadeczky.tamas@uni-nke.hu
[2] Solms, Rossouw von, Niekerk, Johan van, From information security to cyber security, Computers & Security, Volume 38, 2013, Pages 97-102, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2013.04.004.
[3] Leuprecht, Christian, Skillicorn, David B., Tait, Victoria E., Beyond the Castle Model of cyber-risk and cyber-security, Government Information Quarterly, Volume 33, Issue 2, April 2016, Pages 250-257 doi:10.1016/j.giq.2016.01.012

Technology development, as we described above, made local system security improvements indispensable.[4] In case of e-government systems, a higher level of the problem also exists: attack against multiple systems or against a full infrastructure. This can take part of a conventional war, as cyberwar or may be an unconventional event, called cyberterrorist attack; they are all part of cybersecurity. Thus a major part of cybersecurity can be only handled with governmental or supranational level, with cybersecurity strategies,[5] legal regulation, and dedicated authorities.
Table 1 shows the changes in the EU and in Hungary parallelly, which will be detailed in this article.

Year	The European Union	Hungary
2004	Regulation on establishing ENISA	
2012		National Security Strategy
2013	EU Cybersecurity Strategy The new regulation on ENISA	National Cybersecurity Strategy Governmental Information Security Act
2016	NIS directive	
2017	Cybersecurity Act (proposal)	National Cybersecurity Strategy (change proposal according to NIS)

Table 1: Legal regulations about cybersecurity in the EU and Hungary

2. Cybersecurity strategy in the EU

Before forming any exact strategy, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency* came into force. The regulation established ENISA, with the following objectives:

- *The Agency shall enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems.*

- *The Agency shall provide assistance and deliver advice to the Commission and the Member States on issues related to network and information security falling within its competencies as set out in this Regulation.*

- *Building on national and Community efforts, the Agency shall develop a high level of expertise. The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors.*

[4] Szádeczky, Tamás. The role of technology. Auditing and certification in the field of data security. In.: Gergely László Szőke (ed.): Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary, HVG-ORAC, Budapest 2012, pp. 311-337.
[5] James A. Lewis, National Perceptions of Cyber Threats, Strategic Analysis, 38:4, 2014, 566-576, doi:10.1080/09700161.2014.918445

- *The Agency shall assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security.*

It is important to remark the verbs used: enhance, provide, develop, and update. They show us the aim to form a soft agency without policy-making power. The exact plans with ENISA were also unclear.[6]

The tasks aligned with the objectives above were the followings:

- collect appropriate information to analyze current and emerging risks
- provide advice to stakeholders
- enhance cooperation between different actors
- facilitate cooperation the Commission and the Member States
- contribute to awareness raising
- assist the Commission and the Member States in their dialogue with industry
- track the development of standards
- advise the Commission on research
- promote risk assessment activities,
- contribute to Community efforts to cooperate with third countries
- express its own conclusions independently,

As we see from the list above, the tasks are supportive functions. There are no regulatory, standardization or audit functions dedicated to ENISA. In contrast to the field of data protection, the European Data Protection Supervisor has authority to audit EU organizations.

The bodies of ENISA are the Management Board, the Executive Director, and the Permanent Stakeholders' Group.

The first official cybersecurity strategy in the European Union was formed with the Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union. It's the Open, Safe and Secure Cyberspace formed on the 7th February 2013.

The strategy defined five strategic priorities, which address the challenges:

[6] Hearn, J. (2003). Moving forward? Security & Privacy, 1(2), 70–71.

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyber defense policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

In the first strategic priority, achieving cyber resilience, the need to modernize and strengthen ENISA was articulated.[7]

After nine years of ENISA's operation and providing nearly 300 publications, with focus topics incident- and risk management, critical infrastructure protection, trust services and computing cloud, a new regulation came into force. Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21st May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 has changed the objectives:

- The Agency shall develop and maintain a high level of expertise.
- The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security.
- The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.
- The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.
- The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors.

The tasks were also changed according to the objectives:

- support the development of Union policy and law, by advising, providing preparatory work, analyzing

[7] Ruohonen, Jukka, Hyrynsalmi, Sami, Leppänen, Ville, An outlook on the institutional evolution of the European Union cyber security apparatus, Government Information Quarterly, Volume 33, Issue 4, October 2016, Pages 746-756 doi:10.1016/j.giq.2016.10.003

- support capability building by supporting the Member States, promoting voluntary cooperation, assisting by supporting the operation of a Computer Emergency Response Team (CERT) for them;

- supporting the raising of the level of capabilities of national/governmental and Union CERTs, including by promoting dialogue and exchange of information, with a view to ensuring that, with regard to the state of the art, each CERT meets a common set of minimum capabilities and operates according to best practices;

- support voluntary cooperation

- cooperate with Union institutions, bodies, offices and agencies,

- contribute to the Union's efforts to cooperate with third countries and international organizations

The most important change in the tasks was the establishment of CERT-EU,[8] as a new service, and also a part of Computer Security Incident Response Teams (CSIRT) network according to NIS directive.[9] Incident management became more important in the operation of ENISA with these changes than in 2004. The incident management theory and practice are very wide; they include the range from operational procedures to governmental response. Illustrative key topics are ISO/IEC 27035, ITIL-based incident response, forensics, and operation of CSIRTs.[10]

The only change in the organization was the staff's addition to the Executive Director, and the Management Board shall establish an Executive Board.

In 2016 the European Commission adopted the Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final. The document dealt with the making the most of NIS cooperation mechanisms and moving towards ENISA 2.0. The section also mentions European Cybercrime Centre (EC3) at Europol as a possible cooperation partner. The Commission is required to evaluate ENISA by 20 June 2018 but plans to do it earlier.

So that a future change is foreseeable with the 2017/0225 (COD) Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency," and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). The voting is forecasted to June 2018. The objectives of ENISA changed slightly:

- *The Agency shall be a center of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers and the information it provides, the transparency of its operating procedures and methods of operation, and its diligence in carrying out its tasks.*

[8] Website of CERT-EU is accessible at https://cert.europa.eu/
[9] Directive (EU) 2016/1148 Article 12. Par. 2.
[10] Tondel, Inger Anne, Line, Maria B., Jaatun, Martin Gilje, Information security incident management: Current practice as reported in the literature, Computers & Security, Volume 45, September 2014, Pages 42-57 doi:10.1016/j.cose.2014.05.003

- *The Agency shall assist the Union institutions, agencies, and bodies, as well as the Member States, in developing and implementing policies related to cybersecurity.*

- *The Agency shall support capacity building and preparedness across the Union, by assisting the Union, Member States and public and private stakeholders in order to increase the protection of their network and information systems, develop skills and competencies in the field of cybersecurity, and achieve cyber resilience.*

- *The Agency shall promote cooperation and coordination at Union level among the Member States, Union institutions, agencies and bodies, and relevant stakeholders, including the private sector, on matters related to cybersecurity.*

- *The Agency shall increase cybersecurity capabilities at Union level in order to complement the action of Member States in preventing and responding to cyber threats, notably in the event of cross-border incidents.*

- *The Agency shall promote the use of certification, including by contributing to the establishment and maintenance of a cybersecurity certification framework at Union level in accordance with Title III of this Regulation, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus strengthen trust in the digital internal market.*

- *The Agency shall promote a high level of awareness of citizens and businesses on issues related to the cybersecurity.*

The tasks improved heavily: the task list consists of 60 elements, grouped into the following seven articles:

- Tasks relating to the development and implementation of Union policy and law

- Tasks relating to capacity building

- Tasks relating to operational cooperation at Union level

- Tasks relating to the market, cybersecurity certification, and standardization

- Tasks relating to knowledge, information and awareness raising

- Tasks relating to research and innovation

- Tasks relating to international cooperation

Furthermore, on 13 September 2017, the President of the European Commission, Jean Claude Juncker announced an implementation toolkit for the Network and Information Security Directive; and a report to ensure an effective response in case of cyber-attacks in the Member States.

3. Cybersecurity organization in Hungary

The first comprehensive security and defense policy system of Hungary after the political change in 1989 did not recognize cyber threats. Neither the National Assembly resolution no. 94/1998 (XII. 29.) on the security- and defense policy principles of Republic of Hungary, nor the Government resolution no. 2073/2004. (IV. 15.) on the National Security Strategy of the Republic of Hungary, nor the Government resolution no. 1009/2009. (I. 30.) on the National Military Strategy of the Republic of Hungary included cyber defense as an objective. According to these policies and strategies, the defense against cyber attacks was treated individually, even in the legal regulation.

Before the Act on Electronic Public Service (before 29 June 2009) there was no acts dealing with information security in public- or governmental networks.[11]

Only the following Government decrees regulated the field:

- 195/2005 (IX. 22) Government Decree on security, interoperability and uniform use of electronic administration systems
- 84/2007 (IV. 25) Government Decree on security requirements of the Central Electronic Service System and related systems
- 193/2005 (IX. 22) Government Decree on detailed rules for the electronic filing
- 194/2005 (IX. 22) Government Decree on requirements for electronic signatures and the associated certificates used in the administrative proceedings, as well as requirements for certification service providers issuing the certificates
- 182/2007 (VII. 10) on the regulation of the central electronic service provider system

These provided security rules sporadically to some systems, without any general framework.

As a result, we may say that relatively low awareness of the legislator and the business is observable in the usage of international IT security standards, despite its significance and the high risk in some areas. No obligations were found in acts of Hungarian Parliament for enforcement of standards in IT security. There have been built-in self-control procedures in some acts, but in practice, those procedures actually haven't worked efficiently.[12]

In 2009 a small change was commenced with the adoption of Act LX of 2009 on electronic public services. It has highlighted the requirement of security as a basic principle.

Organizations providing ICT based public services ensure the publicity of data of public interest (according to the Act on data protection and freedom of information) and protection of personal and any other data during the provision of services.[13]

---

[11] Dedinszky, Ferenc, Informatikai biztonsági elvárások (Information security requirements), MeH-EKK, Budapest, 2008, p. 4.
[12] Szádeczky, Tamás. Information Security - Strategy, Codification and Awareness. In: András Nemeslaki (Ed.): ICT Driven Public Service Innovation. Comparative Approach Focusing on Hungary. Budapest, 2014. pp. 109-122.
[13] Hungarian Act LX of 2009 on electronic public services

During the provision of services, particular attention must also be paid to the fulfillment of realization of information rights, protection of classified information, business secrets and other protected data groups. Service providers ensure IT security, including the integrity of electronic records, and applicability of the electronic signature technology. The legislator refers to the application of electronic signature technology and the importance of compliance with the relevant security requirements.

The use of electronic signatures, according to Act on electronic signature (hereinafter Eat.) can greatly assist in maintaining the integrity of data. However, a huge discrepancy is noticeable between theoretical principles and practice. Despite the above rules, electronic signatures are still not widely adopted and rarely used in such systems.

Service providers shall also ensure the operational continuity and enforcement of information system collaboration requirements. As we have shown in chapter 4 and chapter 5 interoperability, i.e., cooperation between the various systems has particular importance in the government information technology, as island-like systems have been developed, and over time the demand of integration increased fairly. The negative impact of island-like development is still being felt in the area of interoperation. The continuity of operation, as one of the main requirements for IT security, including disaster and business continuity planning, is an important feature for large government databases, where data loss could and would be catastrophic.

Data transmitted to the central system profiling (analysis of user habits, personal information and direct access to meaningful case data) is not allowed according to these regulations. Compliance is ensured with the central system operator by means of technical solution. Profiling, one of the most challenging privacy issue in recent years is declared to be prohibited by a principle in Act LX of 2009 on electronic public services, and the information system must ensure this technically (e.g., through Privacy by Design technologies).

Use of remote services required a face-to-face pre-registration or an equivalent measure and given that a significant number of electronic public services are administrative procedures, they need proper identification. Personal appearance and identification mean a registration in governmental offices or registration by electronic signature.

Authenticity, quality, operational security and confidentiality of the data processed in electronic public services operate under the Central System must comply with defined rules. Here the act refers to Government decree no. 223/2009 (X. 14) about the security of electronic public services. In that, the requirements and procedures were determined in sections from 11 to 32. Requirements set out in the Act are detailed in the following regulations:

- Government Decree 223/2009 (X. 14) on the security of electronic public services
- Government Decree 224/2009 (X. 14) on the central electronic system service's recipient identification and authentication services
- Government Decree 225/2009 (X. 14) on electronic public services and their use
- Government Decree 78/2010 (III. 25) on requirements of electronic signatures in administration and certain rules for electronic communication

There was a bill on information security in 2009, which never came to force, but had a remarkable impact on the area.[14] The proposal was a draft legislation framework, a so-called lex specialis.
The bill's scope was all IT systems and services in the Republic of Hungary, including private computers. It would have been applied to the operators and users, also.

According to this information systems are to be divided into 5 separate security level. One of the factors of the grouping was storage of personal data. The groups were the followings:

- Level 1: home computer networks and individual computers connected to the Internet
- Level 2: information systems used by every legal relationship between employer and employee, internal IT network, limited internal access non-public electronic communications services or internal network or individual computer capable of using public electronic services
- Level 3: any public electronic services that don't handle, store, process or transfer personally identifiable information, including anonymous registration services
- Level 4: organizations providing public electronic services, application service provider and it's public electronic services, regardless of personal data processing; any public electronic services that handle, store, process or transfer personally identifiable information
- Level 5: critical infrastructure sector's computer system, closed-circuit, and public electronic network or services and information technology

One of the most interesting questions is the mandatory audit required at level 4-5 as a mean of control. According to the original intention, this control would have been conducted by audit firms which are accredited previously by the National Accreditation Body for Certification Activity. Creators of the legislation could not specify whether that responsibility belongs to management systems or product certification.

Most importantly, the social impact of the law would have been significant, at least because of its wide scope. Critics had said there was lack of audit control in level 1 to 3, which made it a redundant regulation. In contrast to that, the legislation could have set the level of security requirements under other laws, because of its lex specialis character. For example, in Criminal Code Section 423 *adequate protection* is required in the case of hacking, but it was not defined earlier. The new law might have given meaningful content to it, and increasing legal certainty.

Government Decision no. 1035/2012 (II.21.) on Hungary's National Security Strategy required the strengthening of the security of electronic information systems to enhance the protection of critical national information infrastructure, and the development of the adequate cyber defense.

Stemming from this statement of the National Security Strategy, the Government adopted the Government Decision no. 1139/2013 (III. 21.) on Hungary's National Cybersecurity Strategy. The main objective therein:

- Establish incident reporting mechanisms
- Establish an incident response capability

[14] MeH, Draft of act on information security, 2009.

- Engage in international cooperation
- Strengthen training and educational programs
- Establish baseline security requirements
- Organize cyber security exercises
- Critical Information Infrastructure Protection
- Develop national cyber contingency plans
- Establish an institutionalized form of cooperation between public agencies

The legislator took the view that recently experienced cyber wars worldwide justified the coding of a modern Hungarian Information Security Act and on 25th April 2013 was a huge milestone for the administrative control of information, when Act L of 2013 on the electronic security of state and local government organizations was published.

The scope of the act, despite its title and scope definition in Section 2, is significantly wider as it seems to be,[15] mainly because of the following extensions: data processors of national data assets, European critical infrastructure system elements, national critical infrastructure system elements, as defined by law. These bodies can significantly extend the scope (even with private companies), so typically the public utility providers, electronic communications services, financial organizations could be included. An itemized list has not been published at the time of writing this manuscript. The law prescribes the essential items known as CIA triad (confidentiality, integrity, and availability) in information security field.

The Act requires the integrity and the availability of information systems in a closed, complete, consistent way, proportionate to the risks for the electronic system and components. It is important to explicitly include the security control implementation's proportionality to risks and use of risk assessment in the state information security requirements, because security measures are typically implemented in an ad hoc manner, to minimize security budgets.

In order to protect electronic information systems and data, proportionally to the risks, the Act states that the electronic information systems must be allocated to particular security classes. This classification is based on confidentiality, integrity and availability properties on a scale of 1 to 5, where 5 is the highest security level. From this section of the Act it seems that each part of CIA factors has to be evaluated separately, but from other parts of the Act, we don't find this distinction.

Although the security classification depends primarily on the security classification of information, the law, in contrast to the earlier bill, does not specify what minimal security controls should be applied to data. In contrast, in Section 9 (2) it determines the minimum security level classification for a variety of organizations. This probably will have the consequence that the security needs of data will not be evaluated. Instead, it will be adjusted to the security levels according to the minimum-list since public sector tries to spend as few as possible on security. According to the Act

[15] Muha, L., Krasznay, Cs., Kibervédelem Magyarországon: áldás vagy átok? (Cyber defence in Hungary: Bless or curse?), HWSW ONLINE, 2013: Paper 5026.

Section 7 para 5, in *exceptional circumstances*, the manager of the organization may set a lower security class, which is another easier way to avoid spending on security. The only thing that can stop this expected downward bidding, the strictness of National Electronic Information Security Authority, based on Section 9 Para 4. The authority is formed by Act Section 14 Para 1.
The minimum grades in the Act per organizations according to Section 9 Para 2:

- Level 1: no organizations (no requirements at this level)
- Level 2: Office of the President, Office of the National Assembly, the Constitutional Court 's Office, Office of the Commissioner for Fundamental Rights, local and national self-governmental bodies, the administrative authority associations
- Level 3: central state administration bodies, the National Judicial Office, courts, prosecutors' offices, the State Audit Office, National Bank of Hungary, the capital city and county government offices
- Level 4: Hungarian Defense Forces
- Level 5: data processors of national data assets, European critical infrastructure system elements, national critical infrastructure system elements, as defined by law

As we mentioned earlier, the law does not define what these security levels are, or how should the classification be conducted and what the detailed rules for the levels are.

According to Section 11 Para 1 (c), the head of the organization is obliged to appoint a person in charge of the electronic information system security, who is responsible for tasks related to the protection of electronic information systems. The list of tasks includes responsibilities of a conventional chief information security officer (CISO). Its name and definition are suggesting that this person exempt the head of the organization and its employees from their security-related task, but this shouldn’t be the case.

The Act set up the National Electronic Information Security Authority under the Ministry of National Development. As a specialized authority, National Security Authority is involved in their activities with forensic log analysis and vulnerability testing. The existing Government Computer Emergency Response Team (GovCERT) responsibilities have been migrated to the Special Service for National Security. According to Section 23, the National University of Public Service developed training for those responsible for the security of electronic information systems and staff organizations.

After changes of political forces in the government, the topic of cybersecurity was handed over to Ministry of Interior with the Government Decree 187/2015. (VII. 13.). Thus the National Cyber Defense Institute formed in the Special Service for National Security with the following elements:

- administration by National Electronic Information Security Authority
- incident management and response by GovCERT-Hungary
- forensic log analysis and vulnerability testing by National Security Authority

This is also the actual setup as of January 2018. National Cyber Defense Institute is planned to be competent national authority according to NIS.[16] There are four designated CSIRTs:[17] LRLIBEK for critical infrastructures, operated by National Directorate General for Disaster Management, Ministry of the Interior, MILCERT operated by the Military National Security Service, Hun-CERT the Hungarian Computer Emergency Response Team for Council of Internet Service Providers operated by the Hungarian Academy of Sciences Institute for Computer Science and Control, and NIIF-CSIRT, which is the Computer Security Incidents Response Team of NIIF/HUNGARNET, the Internet provider of universities, higher education institutes, some secondary schools, academical research organisations and non-profit institutions in Hungary operated by National Information Infrastructure Development Institute.

4. Conclusion

ENISA was established in 2004 as a consultative body. Both the EU and the Hungarian Cybersecurity Strategy was accepted in 2013. The strategies implied changes in the treatment of cybersecurity topic at the higher level. The objectives and tasks of ENISA have been changed, and the Hungarian authority was formed that year. The next hop was the NIS directive and its implementation in the member states' law, which also provides reinforcement to EU legislation to improve ENISA.

One of the main objectives and tasks both for ENISA and in the Hungarian regulation is the training. Even in the private sector, there is a huge need for well-trained IT personnel. The required level of training is much higher in the cybersecurity, and also real-life laboratories shall be used for such training.[18]

Another aspect of cybersecurity is the military or cyber warfare field. Many EU members, as well as Hungary, is a NATO member, which shapes our defense politics more than the EU Common Security and Defense Policy. NATO recognized cyberspace as a 'Domain of Operations' at Warsaw Summit in 8-9 July 2016. In fact, there are also no elements, which are directly applicable at the member level. But the thing that cyberspace became the fifth domain of operation, and the requirement that all military operations shall include operations will have a positive effect on the defense.

More changes happened in the previous years in the European legislation, and therefore preparedness to cybersecurity risk is much better nowadays, but we are lagged behind the United States of America and behind China.[19] Thus there is a long way to go.

[16] Article 8 of Directive (EU) 2016/1148
[17] According to Article 8 of Directive (EU) 2016/1148
[18] Dominguez, Manuel, Prada, Miguel A., Reguera, Perfecto, Fuertes, Juan J., Alonso, Serafin, Moran, Antonio, Cybersecurity training in control systems
using real equipment, IFAC PapersOnLine 50-1 (2017) 12179–12184, doi:10.1016/j.ifacol.2017.08.2151
[19] Krzysztof Feliks Sliwinski, Moving beyond the European Union's Weakness as a Cyber-Security Agent, Contemporary Security Policy, 35:3, 2014, 468-486, doi:10.1080/13523260.2014.959261

5. References

[1] DEDINSZKY, F., Informatikai biztonsági elvárások (Information security requirements), MeH-EKK, Budapest, 2008, p. 4.

[2] DOMINGUEZ, M. et al., Cybersecurity training in control systems using real equipment, IFAC PapersOnLine 50-1 (2017) 12179–12184, doi:10.1016/j.ifacol.2017.08.2151

[3] HEARN, J. (2003). Moving forward? Security & Privacy, 1(2), 70–71.

[4] LEUPRECHT, C. et al., Beyond the Castle Model of cyber-risk and cyber-security, Government Information Quarterly, Volume 33, Issue 2, April 2016, Pages 250-257 doi:10.1016/j.giq.2016.01.012

[5] LEWIS, J. A., National Perceptions of Cyber Threats, Strategic Analysis, 38:4, 2014, 566-576, doi:10.1080/09700161.2014.918445

[6] MUHA, L., KRASZNAY, Cs., Kibervédelem Magyarországon: áldás vagy átok? (Cyber defence in Hungary: Bless or curse?), HWSW ONLINE, 2013: Paper 5026.

[7] RUOHONEN, J., HYRYNSALMI, S., LEPPÄNEN, V., An outlook on the institutional evolution of the European Union cyber security apparatus, Government Information Quarterly, Volume 33, Issue 4, October 2016, Pages 746-756 doi:10.1016/j.giq.2016.10.003

[8] SLIWINSKI K. F., Moving beyond the European Union's Weakness as a Cyber-Security Agent, Contemporary Security Policy, 35:3, 2014, 468-486, doi:10.1080/13523260.2014.959261

[9] SOLMS, R., NIEKERK, J., From information security to cyber security, Computers & Security, Volume 38, 2013, Pages 97-102, ISSN 0167-4048, doi:10.1016/j.cose.2013.04.004.

[10] SZÁDECZKY, T., Information Security - Strategy, Codification and Awareness. In: NEMESLAKI, A., (Ed.): ICT Driven Public Service Innovation. Comparative Approach Focusing on Hungary. Budapest, 2014. pp. 109-122.

[11] SZÁDECZKY, T., The role of technology. Auditing and certification in the field of data security. In.: Gergely László Szőke (ed.): Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary, HVG-ORAC, Budapest 2012, pp. 311-337.

[12] TONDEL, I. A., LINE, M. B., JAATUN, M. G., Information security incident management: Current practice as reported in the literature, Computers & Security, Volume 45, September 2014, Pages 42-57 doi:10.1016/j.cose.2014.05.003

BIG DATA AND ALGORITHMS IN THE PUBLIC SECTOR AND THEIR IMPACT ON THE TRANSPARENCY OF DECISION-MAKING[1]

Gergely László Szőke[2]

DOI: 10.24989/ocg.v331.25

Abstract
Big Data is clearly one of the most used buzzwords nowadays, but it really seems that the phenomenon of Big Data will have a huge effect on many different fields, and may be regarded as the new wave of the information revolution started in the 60s of the last century. The potential of exploiting Big Data promises significant benefits (and also new challenges) both in the private and the public sector – this essay will focus on this latter.

After a short introduction about Big Data, this paper will first sum up the potential use of Big Data analytics in the public sector. Then I will focus on a specific issue within this scope, namely, how the use of Big Data and algorithm-based decision-making may affect transparency and access to these data. I will focus on the question why the transparency of the algorithms is raised at all, and what the current legal framework for the potential accessibility to them is.

1. Big Data – the new wave of information revolution

The expression of "Big Data" is definitely one of the most used buzzwords in any discussion about recent technological development. Despite or besides the "Big Hype" about Big Data[3] it really seems that this revolution "will transform how we live, work, and think".[4] The recent tendencies can be regarded as the new wave of the information revolution started in the 1960s.

The Big Data phenomenon has many faces, no comprehensive definition is used – the approach by IT experts and tech companies, by economists or by lawyers may be different. Still, there are some common cornerstones to describe the Big Data tendencies: the industry uses the so called 3-4-5 (or even more) "Vs", as decisive features:[5] (1) Volume refers to the enormous and fast increasing

1

SUPPORTED BY THE ÚNKP-17-.4. NEW NATIONAL EXCELLENCE PROGRAM OF THE MINISTRY OF HUMAN CAPACITIES

[2] Assistant professor and head of the Group of ICT Law, Department of Administrative Law at the Faculty of Law, University of Pécs, and researcher of the Big Data Research Group of the Szentágothai Research Center of the University of Pécs. E-mail: szoke.gergely@ajk.pte.hu

[3] Cf. for instance Steve Dodson: Big Data, Big Hype? https://www.wired.com/insights/2014/04/big-data-big-hype/, but this question has been raised several times in the past years.

[4] Cf. Kenneth Cukier and Viktor Mayer-Schönberger's famous book: „Big Data: A Revolution That Will Transform How We Live, Work, and Think" (2013, Houghton Mifflin Harcourt)

[5] Cf. Gartner's definition containing volume, velocity and variety (https://www.gartner.com/it-glossary/big-data), the IBM's approach of 4V (http://www.ibmbigdatahub.com/infographic/four-vs-big-data, which was later completed with the fifth V of „Value" (https://www.ibm.com/blogs/watson-health/the-5-vs-of-big-data/), and even complemented with Variability and Visualisation (by Eileen McNulty http://dataconomy.com/2014/05/seven-vs-big-data/)

amount of data; (2) Variety means the diversity of the data (including the fact that most of the data are unstructured, and could hardly be processed with the "old" data mining techniques); (3) Velocity refers to the fact that both the appearance of any new data and the expected analysis of these data are very fast (often real-time); and (4) Veracity points to the uncertainty of data.

Data alone are not enough, of course, so the main issue is how to analyse them. Not surprisingly new data mining technologies and powerful algorithms have emerged recently to solve this problem, including self-learning algorithms, which may "develop" by themselves, if enough data are available for them. But the operation of the algorithms is often described as a "black box". First, the actual way how they work is not understood by average people, and, besides this, the algorithms are usually treated as a treasured trade secret of the tech companies. Moreover, machine-learning mechanisms may pose a further risk, since their operation and their results are often inscrutable at times even for their programmers [5, p. 10].

Some general consequences of the spread of Big Data analytics are predictable. As Cukier and Mayer-Schönberger summarize it, first of all, no sampling of data will be necessary, since all (or almost all) data can be analysed – as they refer to it, using the terminology of statistics, "n = all". Once we have so many data, no clear hypotheses or straightforward questions are needed. This also means that unexpected and surprising correlations may be revealed. Another consequence – say Cukier and Mayer-Schönberger – may be the shift from causation to correlation: Big Data analysis only answers the question: "what", but says nothing about "why", but in many situations this is far enough [6, pp. 30-32]. Finally, and from a legal and ethical point of view this seems to be the most important one, Big Data analysis tends to be used for predicting future actions and behaviours with a considerable degree of probability (and predictions can be easily used for manipulation and nudging) [25, p. 25].

Generally, it seems that exploiting the potentials of Big Data holds out unprecedented business opportunities and benefits for the society as a whole, but also gives rise to new risks and challenges, of course. The potential spheres of usage are almost endless: development of new products and services, more effective (online) marketing and sales activity, health care, energy networks, transport and traffic systems, journalism, crime prevention and investigation, urban development, or gaining new scientific results, etc.

2. Big Data in the public sector

2.1. Potential use of Big Data and algorithms in the public sector

It is quite avowed that the activity of the public sector is based on data: using information is deeply embedded in the services provisioning, inspection and policy-making activity [14, p. 363]. So any changes (mainly if these changes seem to be radical) in the way of managing data shall significantly affect the operation of the public bodies.

As for the positive effects, Big Data analytics in the public sector may result in smarter data management, more effective (evidence-based) decision-making, personalized public services, better predictive analysis and problem solving [11, p. 386], and it may reduce fraud and corruption, increase transparency [20, p. 289], – so generally more productivity and efficiency is expected. These are more or less the same opportunities that come up in the business sphere.

Although there are some driver factors, there are also significant constraints of the spread of Big Data analytics in the public sector, like the lack of political willingness, lack of skilled people or legal uncertainties and concerns [18, p. 199]. Still, if we have a look at the relevant literature, we may find many examples and efforts for the usage of Big Data and algorithms in the public sector from all over the world: some of these are only plans or intentions, some others are in a pilot program phase and there are also examples for everyday use. Before looking through these examples and ideas, it has to be noticed that some of them have emerged in countries with a much lower level of privacy protection compared to the strict European data protection regime. However, I find it useful to show these tendencies too, to make the potentials (including the potential risks) of Big Data analytics more tangible.

1. Analysing traffic and transport data. Big Data analytics is often used for making traffic and transport systems more effective. In Brazil, for example, the continuous monitoring of traffic and road conditions helps to reduce the time to identify traffic problems from several hours to several minutes and assists in prioritizing road repairs. In Japan, an integrated system is designed to resolve traffic problems, like traffic congestion and accidents [11, p. 387]. If we use our fantasy, many other solutions can be imagined (some of these are likely to be used somewhere): analysing the data of all passengers and travels may help fine-tuning the mass-transit system (e.g. instant decisions on starting another bus or tram), analysing of real-time traffic data may help using intelligent traffic lights, or – by analysing the bigger picture – may help decide where a new road should be built or which older one should be reconstructed.

2. Improving health care services. Big Data holds out great opportunities both for more effective medicine and for improving the health care system itself. Analysing a huge amount of data may help detecting harmful (or even deadly) drug interactions [4], and may improve personalized medicine [1]. Predictive analysis, as it has been tried in Australia, may help in the hospitals' resource management, such as bed management, staff resourcing, and scheduling of elective surgery, but even the workload of an emergency department can be predicted with an accuracy of up to 93% [11, 13].

3. Fighting against tax fraud and corruption. We may find some examples that new data mining technologies are used in tax administration [22] and fighting against corruption, which seems to be reasonable, since a quite complex approach and analysis of a wide range of data is needed in these fields. There was, for instance, a Hungarian pilot program for using text-mining methods to analyse text-based public databases (procurement database, company registry, legal databases and publicly available other sources, like forums, blogs, and social media activity) in order to find fraudulent practices in the public procurement processes. The semi-automated system helped to find signs of suspicious behaviour, like invalid bids, co-ordinated high prices, geographically based market co-ordination, suspiciously similar prices or tenders, etc. [23].

4. Big Data for crime prevention and in criminal procedures. It is generally accepted that prevention is always better than reaction. Using Big Data methods makes predictive policing available, where historical (crime) data is used to discover trends and patterns, which might allow more effective and efficient deployment of police forces [18, p. 198]. Former data may be used to predict the location and time of a future crime likely to be committed, including identifying endangered zones [6, 19]. However, prediction may be used for a single person too. In some states of the United States software algorithms are used to assess some risks regarding the defendants, like pre-trial risks and risks of re-offending – and this information is used in the procedure or in the final judgement by the court [8, 15]. We could also find examples for actions taken against people before

committing a crime. In 2014, the "Chicago Police Department sent uniformed officers to make »custom notification« visits to individuals," because they had been identified by a software as people likely to commit a crime. "The idea was to prevent crime by providing them with information about job training programs, or let them know about increased penalties for people with certain backgrounds" [17]. Besides these examples of predictive analysis, it is important to see that Big Data methods are also used in the course of the investigation, e.g. for mapping the complex connection graph of the suspect [19, p. 192].

5. Fighting against unemployment. At first glance, it is not an obvious field of use, but we may find some examples for using Big Data and algorithms to reduce unemployment. In Germany, the historical customer data (including profiles) were analysed by the German Federal Labour Agency in order to offer more personalized services for unemployed people [11, p. 387, 18, p. 198].

6. Big Data in education. Among many other possible fields, algorithms may be used for complex evaluation of students' school performance [9, p. 1], but, on the other hand, also for analysing a mass of social media messages in order to get a real picture about the students' satisfaction with their courses and teachers [21, p. 17].

7. Analysing environmental data. Mass collection and analysis of environmental data may happen for several reasons. In India, for instance, real time monitoring of water flow is planned to minimize unaccounted water by detecting large changes in water flow [11, p. 387]. In the United States, algorithms help asses "the risks children face from exposure to lead at hazardous waste sites". A software for weather forecasts also uses a huge amount of data and sophisticated algorithms [9, 12].

These more or less randomly collected examples clearly show the relevance of Big Data analytics in the public sector in a very wide range and in divergent fields of use. It is clear that the public sector may win much by using the new technologies, but some of the examples might also remind us about the potential risks and challenges.

2.2. Risks and challenges

Using Big Data and algorithmic decisions may give rise to many ethical and legal concerns. If we think about taking any kind of actions against a person who is only predicted to commit a future crime or the fact that Big Data analysis may easily reveal hidden, surprising correlations and new information "never asked for", the alarm is surely sounding in many lawyers' heads.

The rich legal literature on these issues focuses – besides some others – mainly on discrimination, on privacy concerns, (both are very important and valid, but not the subject of this paper now), and on transparency and accountability for the algorithmic decision making. I am going to continue with this latter issue.

3. Big data and transparency of algorithmic decision-making

Although it seems at first glance that everyone may have easy access to information via the Internet and online services, access to the Big Data (meaning access to a huge amount of data), and especially, access to the new data analysing technologies and algorithms is actually limited. The present era "is characterized by an increasing concentration of the control over the information in the hands of a limited number of private and public entities, which, in different cases, cooperate in

sharing information with each other to increase their position as owners and gatekeepers of knowledge" [16, p. 23]. The imbalance of the informational power seems to be bigger than ever.

I collected many fields of use of Big Data analytics and algorithms in the public sector, providing some actual examples. It is quite clear that the results of any decision based on these new methods and techniques may significantly affect the life of a single person or a smaller or bigger community, but sometimes also the whole society.

Theoretically, it may have many advantages if the decision is based on a huge amount of real data and on smart algorithms. First, it seems that the exclusion of human nature may lead to a more objective and unbiased result. In many cases this is far from true, and the algorithms may contain biases. This may be "pre-existing", which means that if the used data show a discriminatory practice, the algorithm will "learn" this and use it as a standard. There may also be hidden problems in the code itself, which may lead to biases, and these may be invisible even for the programmers [9, p. 2].

Another problem that may arise is that the use of Big Data and algorithms may show surprising, unexpected results, usually only showing the correlation without justified causality. How can these kinds of "unjustified results" be accepted by the subject of the decision? [24, p. 108]. How can someone challenge a decision which is not based on reasons, only on correlations, especially if the way how the result came up is not known at all?

If the algorithms are not transparent, some further uneasy questions may arise: How is it known that the algorithm is fair and just, and not discriminatory? What are the limits, how is it known when it will break down or fail? What are those data that are excluded or overemphasised by the algorithms? [7, pp. 9-10].

Based on these reasons many argue that algorithms should be more transparent, or somehow controllable, or at least these issues have to be seriously dealt with [7, 9, 10, 16]. On the other hand, it also has to be noted that the development of new and powerful algorithms is the driving force of today's IT innovation, the success of companies nowadays, both that of the big ones and thousands of start-ups, is largely based on the new analysing methods. In my view, it is reasonable to distinguish between the decisions in the business sector and in the public sector. In the business sector the relationship between the partners is – at least theoretically – based on voluntarity, and ideally the market competition works well enough to force business actors to offer the most desirable terms and conditions, including as much transparency as expected by the customers. So generally the decisions of the companies, for example, a bank's decision about a loan based on a scoring system, or about the amount of the insurance fee based on certain personal circumstances [24, p. 108] are not subject to detailed justification by law. Admitting that this is an idealized picture also about the business sector,[6] in the public sector the situation is inherently different. The decisions are usually compulsory for those concerned, and there is no possibility to turn to the "competitor" if the "terms and conditions" are not acceptable. On the other hand, procedural rules are guaranteed by fundamental rights and by detailed legal regulation, and there is a possible remedy and judicial control over the decisions. However, to use any possible remedy, information is needed about the details of the background of the decision, so that is why generally it has to be

[6] Some companies are in a monopoly or quasi-monopoly position (e.g. due to the network effect), or all the actors on the given market basically use very similar data analytics while providing their services, etc.

justified in a written form by the decision making body. As a summary, the transparency of the algorithms seems to be much more important in the public sector than in the business sphere.

Finally, accepting at least the thesis that transparency of the algorithms has to be studied, and seeing that the legal situation concerning the transparency of algorithms is far not obvious, as a first step it is worth to give an overview of the affected legal institutions and instruments. Therefore, I will try to provide a picture of the relevant legal provisions.

4. Current legal framework of the transparency of algorithms

If we are thinking about the transparency and accessibility of certain information (the algorithms) in certain decision-making processes, it is first worth to study their accessibility by the general public, and then the possibility to have access for those who are the subject of the decision.

4.1. Access to algorithms by the general public

The first question worth studying is whether the algorithms on which a decision is based are accessible for the public under Freedom of Information (FOI) Law. The detailed rules of freedom of information and/or access to public documents are not harmonized in the EU, so they may vary in the different countries. So the starting point of the analysis is the Hungarian FOI regime,[7] but my consequences are valid in a much broader sense, since it seems that the basics of FOI Law, namely what is accessible (in most countries the data or information, no matter what medium it is stored on), and the limits of access (national security, personal privacy, commercial confidentiality and internal documents or discussions) are quite similar in the different FOI regimes [3, p. 22].

Katherine Fink made an analysis based on the US FOI Law to answer the question of the accessibility of algorithms. Following her – very logical – structure, first, it is worth to try to answer whether algorithms are a kind of information which is subject to the FOI Law at all and second, to study whether any of the exemptions can be applied to algorithms [9].[8]

Under the Hungarian FOI regime, the subject of the law is "public information", which "shall mean any known fact, data and information, other than personal data, that are processed and/or used by any person or body attending to statutory State or municipal government functions or performing other public duties provided for by the relevant legislation (including those data pertaining to the activities of the given person or body), irrespective of the method or format in which it is recorded, and whether autonomous or part of a compilation."[9] Although the definition is quite wide, it is far not obvious, whether an algorithm used by a public body comes under the scope of this definition.

Even if we accept that the algorithm itself[10] is subject to the FOI Law, still the applicability of some exceptions may arise. First it can be regarded as a "data underlying the decisions" (data for internal use), which may be kept in secret for ten years from the date it was compiled or recorded. It may also be kept in secret after the decision is made, if it supports a future decision as well, or if

[7] Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Infotv.)
[8] She also made an empirical research about whether software and algorithms were provided based on a FOI claim, and found also positive results, when e.g. the used software was an open source one, and its operation could be fully analysed.
[9] Infotv., Sec. 3. 5.
[10] At this time I will not deal separately with the legal status of input and output data, which could form the basis for further study later on.

disclosure is likely to jeopardize the legal functioning of the body or the discharging of its duties without any undue influence.[11] It seems that under the Hungarian Law the algorithms may easily be regarded as "data underlying the decision."

Another limitation to access to public information is trade secret. Algorithms of private companies are typically their treasured trade secrets, so their accessibility is based on the company's decision. If the algorithm is developed by the public body itself (or by another public body), the situation is different, since they cannot generally refer to a trade secret as an exception.

Finally, no data is accessible if it is personal data (with some very limited exceptions). The algorithm itself is very unlikely to constitute personal data, but both the input and the output data may be personal data. In this case, data protection regulations shall apply, which exclude general accessibility, but at least grant access rights for the data subject to their own personal data.

4.2. Access to algorithms by the individual concerned

Decisions on individuals may concern natural or legal persons. If the decision of the public body concerns a natural person, than the access rights under the data protection law shall apply. Besides this, both for natural and legal persons access rights to the documents of the proceeding in question (e.g. public administration procedure, civil procedure or criminal procedure) may be applied.

4.2.1. Data Protection Law

The law on data protection is harmonized in Europe, after 25th May 2018, the new European General Data Protection Regulation,[12] the GDPR shall apply.[13] In the Data Protection Law context two definitions are relevant. One is profiling, which "means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"[14] and the other is "automated decision making", which is not defined generally. Automated decision-making may have two types: (1) the one as defined in Article 22, which refers to "decision based solely on automated processing [without human involvement], including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her", and (2) those automated decisions which do not meet these criteria, whether because they are only partly automated (there are meaningful human interventions), or because they have no legal or similarly significant effect.

Based on the examples summarized above, we can see that in the vast majority of the cases, no fully automated decisions are made, based on profiling, in the public sector, rather human intervention is typical, and the algorithms "only" help the decision maker to decide. Concerning these cases the special rules based on Art. 22 shall not apply. This means that the general data protection rules are applicable supplemented with some special details, based on the interpretation of the general rules.

[11] Infotv., Sec. 27. (5)-(6).
[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
[13] Before that date, the national implementations of the Directive of 95/46/EC (Data Protection Directive) are applicable.
[14] GDPR, Art. 4 (4)

The data subject shall generally have the right to get information before the data processing, and the right of access at any time during the data processing. The obligation covers to provide information about the purposes of the data processing, including the fact that the processing is for the purposes of both profiling and making a decision based on the profile generated; and about the processed data, which means that at least the input data should be made available for the data subject, and some general information about the profile itself. [15] Nevertheless, this does not mean the accessibility of the algorithm itself.

It is not typical (so far) in the public sector that decisions are made without any human intervention, but if the automated decision is solely automated and it has a legal or significant effect on the data subject, more information should be provided. In this case, the data subject has the right to get meaningful information about the logic involved, and about the significance and the envisaged consequences of the decision.[16] According to the Article 29 Working Party, this still does not necessarily mean the disclosure or even the complex explanation of the algorithm, but the data controller "should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision" [2, p. 14].

It is have to be emphasised again that these rules are not applicable to legal persons, even if they are subject to profiling activity and decisions supported by algorithms.

4.2.2. Access to the documents of the proceedings

The second field, applicable both to legal and natural persons is the right to access to the documents of the proceedings in which the person is involved. This field is not harmonized at European level, so the national legislation may vary significantly about the details. Still, it is quite general that the subject of the proceeding has the right to access the relevant documents of the proceeding.[17] This access is far not unlimited, of course. Based on the Hungarian rules, we can see that trade secret for instance may be a reason to limit the access rights of the parties.[18] It is quite common that a software or algorithm, which may help the public body, is a trade secret of a company, or it is under copyright protection. In these cases, the accessibility of the algorithms may be excluded or very limited.

5. Conclusions

The transparency of Big Data and algorithms is and will be a hot topic in legal academic literature, mainly because their relevance is surely going to increase with the evolution of Artificial Intelligence (which is, at this point, mainly based on Big Data and the new analysing methods). In this article, first, the potential usage of these new technologies in the public sector was pointed out, and then we referred to some basic ideas and thoughts about the necessity of making algorithms more transparent.

Then the current legal framework for accessing the algorithms that are used in the course of decision-making by a public body was shown. First, we analysed whether these algorithms are

[15] GDPR, Art. 13, 1., Art. 14. 1., Art. 15. 1. and WP251, p. 23-24.
[16] GDPR, Art. 13. 2. (f), Art. 14. 2. (g), Art. 15. 1. (h)
[17] Cf. in the Hungarian Law, Act CL of 2016 on General Public Administration Procedures (Ákr.) Sec. 33., Act CXXX of 2016 on the Code of Civil Procedure (Pp.) Sec. 162., Act XC of 2017 on the Code of Criminal Procedure (Be.) Sec. 100-102.
[18] Ákr, Sec. 34. Pp. Sec. 163.

accessible under the Freedom of Information regime and second, whether at least those who are affected by the decision have the possibility to have access to the algorithms. The result of this overview has shown that the possibility of access is quite limited in both fields, and it is mainly based upon the decision of the "owner" of the algorithm, or on the decision of the public body. This situation calls for changes: the transparency and accessibility of the algorithms surely has to be improved in the public sector. But the question of "how" will be the subject of another study.

6. References

[1] ALYASS, A., TURCOTTE, M., MEYRE, D., From big data analysis to personalized medicine for all: challenges and opportunities, *BMC Medical Genomics*, 8(33), 2015, https://doi.org/10.1186/s12920-015-0108-y [Accessed 5 December 2017]

[2] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, Adopted on 3 October 2017 (WP251)

[3] BANISAR, D., *Freedom of Information Around the World 2006*, Privacy International, http://www.freedominfo.org/documents/global_survey2006.pdf [Accessed 25 November 2017]

[4] *Big Data Analysis Proves Effective in Identifying Harmful Drug Interactions,* https://www.dicardiology.com/content/big-data-analysis-proves-effective-identifying-harmful-drug-interactions [Accessed 5 December 2017]

[5] *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, Executive Office of the President, May 2016, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf [Accessed 5 December 2017]

[6] CUKIER, K., MAYER-SCHOENBERGER, V., The Rise of Big Data. How It's Changing the Way We Think About the World, *Foreign Affairs*, 92(3), 2013, pp. 28-40. [Accessed 8 December 2017 via HeinOnline]

[7] DIAKOPOULOS, N., *Algoritmic Acccountability Reporting: On the Investigation of Black Boxes*, Tow Center for Digital Journalism, Columbia University, 2014, http://towcenter.org/wp- content/uploads/2014/02/78524_Tow-Center-Report-WEB-1.pdf [Accessed 5 January 2018]

[8] EPIC, *Algorithms in the Criminal Justice System* https://epic.org/algorithmic-transparency/crim-justice/ [Accessed 4 January 2018]

[9] FINK, K., Opening the government's black boxes: freedom of information and algorithmic accountability, *Information, Communication & Society*, 2017, https://doi.org/10.1080/1369118X.2017.1330418 [Accessed 25 June 2017, via Taylor&Francis Online]

[10] FORGÁCS, I., A Big Data, avagy kezdjünk el gondolkodni a közigazgatás új feladatairól [Big Data, or it is time to start to think about the new tasks of public administration], In: FAZEKAS, M., (ed.): *Gazdaság és közigazgatás: tanulmányok Ficzere Lajos tiszteletére*

[Economy and public administration – essays in honour of Ficzere Lajos], ELTE Eötvös Kiadó, Budapest 2015, pp. 123-133.

[11] GAMAGE, P., New development: Leveraging 'big data' analytics in the public sector, *Public Money & Management*, 36(5), 2016, pp. 385-390. http://dx.doi.org/10.1080/09540962.2016.1194087 [Accessed 25 June 2017, via Taylor&Francis Online]

[12] HAMM, S., *How Big Data Can Boost Weather Forecasting*, Wired, 2013. https://www.wired.com/insights/2013/02/how-big-data-can-boost-weather-forecasting [Accessed 12 December 2017]

[13] HOWARTH, B., *Big data: how predictive analytics is taking over the public sector,* https://www.theguardian.com/technology/2014/jun/13/big-data-how-predictive-analytics-is-taking-over-the-public-sector [Accessed 5 December 2017]

[14] JANSSEN, M., HOVEN, J., Big and Open Data (BOLD) in government: A challenge to transparency and privacy? *Government Information Quarterly,* 32(4). 2015, pp. 363-368. https://doi.org/10.1016/j.giq.2015.11.007 [Accessed 14 September 2017, via ScienceDriect]

[15] LIPTAK, A., Sent to Prison by a Software Program's Secret Algorithms Algorithms in the Criminal Justice System, 1st May, 2017., New York Times, https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?_r=1 [Accessed 4 January 2018]

[16] MANTELERO, A., Social Control, Transparency, and Participation in a Big Data World, *Journal of Internet Law,* 17(10) 2014 pp. 23-29. http://staff.polito.it/alessandro.mantelero/JIL_0414_Mantelero.pdf [Accessed 25 May 2017]]

[17] MARR, B., *How is Big Data Used in Practice? 10 Use Cases Everyone Must Read* https://www.bernardmarr.com/default.asp?contentID=1076 [Accessed 10 December 2017]

[18] MUNNÉ, R., Big Data in Public Sector. In.: CAVANILLAS, J., M., CURRY, E., WAHLSTER, W. (Eds.), *New Horizons for a Data-Driven Economy. A Roadmap for Usage and Exploitation of Big Data in Europe*, SpringerOpen, 2016. pp. 195-208. https://link.springer.com/content/pdf/10.1007%2F978-3-319-21569-3.pdf [Accessed 5 May 2017]

[19] NAGY, T., Big Data – új (m)érték a büntetőeljárásban [Big Data – new measure in the criminal procedure], In: VÓKÓ, GY., (ed.): *Tanulmányok Polt Péter 60. születésnapja tiszteletére [Essays in honour of the 60th birthday of Polt Péter]*, HVG-ORAC, Budapest 2015, pp. 186-194.

[20] RACSKÓ, P., Big Data a közigazgatásban [Big Data in Public Administration], In: NEMESLAKI, A. (ed.): *E-közszolgálatfejlesztés [Development of E-Public Services]*, Nemzeti Közszolgálati Egyetem, Budapest 2014.

[21] SZŰTS, Z., YOO, J., Big Data, az információs társadalom új paradigmája [Big Data, the new Paradigm of the Information Society], *Információs Társadalom,* 16(1), 2016, pp. 7-28.

[22] *Tackling tax fraud with Big Data approach*, Atos, 2015. https://atos.net/wp-content/uploads/2017/10/atos-risk-and-bi-whitepaper.pdf [Accessed 18 December 2017]

[23] VADÁSZ, P., A Case Study on Finding Fraudulent Practices in the Public Procurement Process Using Text-Mining Methods from Open Internet Sources. In: BALTHASAR, A., et. al. (eds.): *Central and Eastern European e|Dem and e|Gov Days 2016*, Austrian Computer Society, Wien 2016. pp. 471-480.

[24] ZŐDI, ZS., Jog és jogtudomány a Big Data korában [Law and Jurisprudence in the Age of Big Data], *Állam- és Jogtudomány*, 58(1), 2017, pp. 95-114.

[25] ZŐDI, ZS., Privacy és Big Data [Privacy and Big Data], Fundamentum, 2017/1-2. pp. 18-30.

CYBERSECURITY IN THE EUROPEAN UNION

Andreas Düll, Anja Schoch and Matthias Straub[1]

DOI: 10.24989/ocg.v331.26

Abstract

The coordinated Denial of Service attacks in Estonia 2007, the successful hacker attacks against the German Bundestag 2015 and the increasing number of cyber-crimes challenge the European Union (EU). In order to overcome these challenges the EU initiated a cyber security strategy in 2013. This paper follows up the question, whether the measures of this strategy are adequate in order to tackle the challenges of the cyberspace in modern times and which improvements can be done. The focus will rely on the analysis of the EU's cyber security strategy 2013 as well as its advancement of 2017. The three issues 'cyber resilience', 'reducing cybercrime' and 'cyber defence policy and capabilities' shall be analyzed. The unlimited sphere of the cyberspace, the invisible and barely identifiable opponents and the focus on national regulations seem to be an unsolved dilemma in the EU. After analyzing the current state, the paper shall formulate future recommendations for action to postulate an improved 'pooling and sharing' as well as the coordination and involvement of existing member states' cyber capabilities. The devolution of responsibilities regarding cyber security to the EU stage is desirable in order to increase the European potency, because a divided EU will have great difficulties enforcing its interests over attacking opponents.

1. Introduction

Our world in its globalization process is in constant and ongoing change, which can lead to positive and negative outcomes. Never before has it been so easy to share knowledge and interact online on a global basis. Each smartphone owner in the EU produces and consumes data. The interconnectivity of Europeans grows constantly. Due to digitalization processes everything is more and more linked, from cars via military equipment over to power plants. This connectivity allows a fast and excessive exchange of data, leading to a higher living standard and prosperous economy. However, the growing amount of digital information transactions and the transformation of the virtual world not only lead to more options but to more challenges worldwide. [1] The coordinated Denial of Service attacks in Estonia 2007, the successful hacker attacks against the German Bundestag 2015 and the increasing number of cyber-crimes, challenge the European Union (EU). Due to the growing cyber-threat within the EU member states the European Commission was determined to outline a Cybersecurity Strategy (CSS) in 2013 with the main objective to guarantee the values, norms and principles of the EU on an online level. These premises also maintain in the updated version of 2017. Considering the cyber-threats this paper follows up the question, whether the measures of the CSS are adequate in order to tackle the challenges of the cyberspace in the 21th century and which improvements can be done. Therefore the CSS`s three main focuses, 'cyber resilience', 'reducing cybercrime' and 'cyber defence policy and capabilities' shall be analyzed. After dissecting the strategy regarding the immanent cyber-threats, the paper shall formulate future recommendations for action to increase the European repercussiveness.

[1] Andrássy University Budapest, Pollack Mihály tér 3, H-1088 Budapest; duell.andreas@gmail.com/ anja_schoch@web.de/ matt-straub@gmx.de

2. European Measures and Challenges

The EU's most issued discrepancy is to grant fundamental rights of expression and participation of individuals and countries on one side and at the same time to ensure national security. The combination of protecting states, businesses and citizens without invading into their freedom of rights is the most grievous defiance of cybersecurity on EU level. [2] In order to provide security without violating the freedom of rights, the EU focuses on a defensive alignment in its CSS and waives offensive measures as "hack backs" against cyber-aggressors.

In the following section the measures and goals of the European CSS regarding the cyber defence policy and capability shall be outlined. In another step the question whether the European measures are sufficient to tackle the most important challenges of cyber-threats shall be answered.

2.1. Cyber Resilience

Potential targets of hybrid attacks are the vital functions of a state. These include the economy, precisely those sectors where dependencies exist, the information and communication systems, in particular the cyberspace and the critical infrastructures in the field of finance, energy, health and logistics. Thus, the question of whether one's own systems and structures are sufficiently adaptable and resistant is becoming increasingly important for all states. The security and full availability of critical infrastructures such as water and energy supply is not only a precondition for prosperity, but for life and survival at all. [3]

In the security discourse, resilience refers to societies and political systems. Resilience is therefore the ability of a community or society to cope, adapt, and recover dangers to which it is exposed and its consequences in a timely and effective manner, thus preserving or rapidly restoring vital basic structures and basic functions. This means that resilience must be constantly maintained and re-acquired. [3] In the EU cybersecurity is taken as a cross-sectional task, both in terms of content and institution, and lies at the interface of civil and military cooperation as well as internal and external security, especially in times of crisis. [4]

The European Commission published a report evaluating the European Network and Information Security Agency (ENISA) and a proposal for a regulation establishing an enlarged EU cybersecurity agency. [5] The mandate of ENISA under Regulation (EU) 526/2010 expires on 19.06.2020. [6] In particular, ENISA assists member states in implementing NIS-Directive (EU) 2016/1148 [7] on measures to ensure a high common level of security of network and information systems in the Union. The evaluation identified the resource shortage of ENISA as a key challenge. For effective coordination of the various actors in the EU, ENISA should therefore be developed into an enlarged EU cybersecurity agency with a permanent mandate, a future 125 staff and an annual budget of around € 23 million. [8] In addition, the Commission proposed the introduction of a European cyber security certification system for digital products and services. In doing so, uniform quality labels comparable to the labeling of foodstuffs should contribute to the trustworthiness and safety of consumers. However, according to the Commission's proposal these should initially be distributed only on a voluntary basis. [5] Furthermore the aim is to develop a cybersecurity crisis response mechanism. This should be regularly tested in the form of cyber and crisis management exercises in the member states. In addition, a European cyber security research and competence center will be established to support the development and use of cyber-defence technologies. A pilot center is to be built in 2018. [9] Finally, a Cyber Security Emergency Fund will be set up in the future to support those member states that have properly implemented all

cybersecurity measures required by EU law. The emergency response could be made available to the affected member states similar to the EU Civil Protection Mechanism. [10] However, the Commission's proposals appear vague and sometimes less substantive. The following problems can be identified against this background: In recent years it has become increasingly clear that radically decentralized structures and voluntary cooperation are insufficient to effectively protect critical infrastructure against cyberattacks. Cybersecurity is increasingly understood as a public good that can only be guaranteed through binding legislation. In order to strike a balance between decentralized multi-stakeholder approaches and effective legal protection, a precision of the understanding of resilience would have been required. The Commission's strategy does not contain any comprehensible criteria that could shed light on which instruments should be used in which scenarios and why. There is a risk that member states, under the guise of the new CSS, could hide negligence on their national responsibilities, on domestic coordination and on the provision of financial resources. [11]

While the General Affairs Council, in its November 2017 conclusions on improving cybersecurity in Europe [12] welcomed the Commission's proposals, it also pointed out that the main responsibility remained with the member states. The Council only assigned a coordinating role to the European level and emphasized the need for the complementarity of EU action. This shows that the Commission has indeed given promising ideas in its strategy, but without possessing the relevant competences in the appropriate fields, it is to be feared that the member states will only take note of the ideas without working substantially on needed reforms.

Moreover, institutional fragmentation in cybersecurity still appears to be an unsolved problem. The upgrading and expansion of ENISA's role can contribute to the improved standardization and security of the cyber infrastructure. Nevertheless, the EU is still a long way from bundling all the measures in a single cybersecurity agency: So far, even the role of ENISA vis-à-vis national cyber security agencies in the member states has not been sufficiently clarified. In this context, institutional fragmentation also means that staff and financial resources are not yet sufficiently bundled. In particular, given that IT professionals are difficult to recruit, especially for the public sector, it is crucial for cyber resilience that all member states also provide the proposed measures with sufficient funding, including the financing of the new network of excellence. [11]

Furthermore, the legal harmonization, which would be essential for increased resilience to cyberattacks, is still awaited. [11] The stricter certification of IT products and the verification of the private sector by ENISA are in themselves very useful and important. These measures continue to be based on the principle of voluntariness. This leaves major structural hurdles in the provision and reporting of cyber-attacks. However, with NIS Directive (EU) 2016/1148, significant progress has been made in requiring critical infrastructure providers and operators, such as banks, power plants, hospitals, water or the Internet, to adopt cybersecurity reforms and related investments. In addition, member states are now obliged to set up national reporting systems. [7] The proposal by the Commission to introduce product certification only on a voluntary basis does not appear to be effective in this context. This could undermine the NIS policy and make new threats easy to play due to the lack of legal liability.

2.2. Reducing cybercrime

The increasing information and communication technology, the expanded use of the internet, the ability of using mobile devices have not only led to benefits but to an increasing vulnerability within the European member states. [13] [10]

Referring to the CSS of 2013 "cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target." [10] It includes 'traditional' violations as fraud or identity theft, content-related offenses such as child pornography or racial hatred and attacks towards computers or information systems. Cybercrime activities as stealing critical data, economic espionage or hacking into state-owned information systems became a new threat to all governments and economies worldwide. [10] According to the Center for Strategic and International Studies (2014) cybercrime is stated as one of the top four economic crimes worldwide. [14] In recent years these activities enlarged and are now a growing and profitable industry. [1] Trends flourishing this new industry result from crimes of terrorist actors, ransomware, banking and data gains, fraud, manipulation of payments and virtual currencies. [15] With this in mind it seems impossible to ensure the needed security level in the private and public sector. Member states still play the most important role in maintaining national security and protecting individual rights, but to fight cybercrime they cannot act effectively alone. Therefore the importance of cooperation is unavoidable. [13] [1]

As the CSS states cybercrimes are increasingly dangerous because they result in high profits and mostly have low risks, therefore "cybercrime is a growth industry" [14] which makes it very attractive to use for threatening infrastructure, government institutions or individual data security. The sources of activities mostly result from criminal, politically motivated, terroristic or state-sponsored attacks and focus on vulnerable harming in knowledge societies. [15] Invisible and barely identifiable enemies are becoming more and more dangerous and raise the difficulties of back tracing. [16] [10] The European Cybercrime Centre (EC3) provided an update (2016) on recent threats resulting from cybercrime incidents and the Internet Organized Crime Threat Assessment (IOCTA) highlights the biggest concerns being ransomware, information-stealing malware and banking trojans for EU law enforcement. Cryptocurrencies like Bitcoin have been the main choice to use for cybercrime activities and services. Furthermore increasing attacks against information systems or phishing campaigns can be reported by EU member states, aiming high value targets as key threat against law enforcement and the private sector. Incidents like the Stuxnet worm, Flame or the Distributed Denial-of-Service (DDoS) attacks against several Estonian national websites show that critical infrastructure can be targeted by viruses and valuable information can be collected. In recent years a large number of malware infections within air-gapped control system networks, combined with the exploitation of zero-day or security vulnerabilities in software programs, got reported across Europe. [17]

The main challenges within the EU are the division of tasks between civil defence, military defence and police, the defence against cyberattacks on critical infrastructures, the quantitative detection of security threats and how deep state security measures can interfere with individual freedom. [15] As one of the main priorities the CSS states the drastic reduction of cybercrime, since there is a high need for the right tools to tackle cybercrime actors and networks. In order to reduce cybercrime the EU suggests a strong and effective legislation in the EU member states, therefore the Budapest Convention[2] as a binding international treaty evolved as a framework for the adoption of guidelines on national level. Since not all member states have the same abilities to tackle cybercrime with effective response, the EU suggests national units as a necessity. Supporting the member states, the European Commission identifies gaps and strengthens capabilities to investigate and combat cybercrime. Connections shall be drawn between the private sector, research institutions and law enforcement to share best practices, new techniques and policy approaches. To reduce cybercrime,

[2] The Budapest Convention of Cybercrime was opened for signature in 2001 and is the most important document on cybercrime and electronic evidence.

the EU has implemented the CSS to focus on legislation and support borderless cooperation. Actions are the facilitation of cross-border access to electronic evidence for criminal investigations and legislative activities. It provides analysis, helps with investigations, creates channels for information sharing and "serves as a voice for the law enforcement community" [10] for all relevant stakeholders fighting against cybercrime. [15] The European Police College (CEPOL) organizes e-learning and training courses in cooperation with Europol to standardize knowledge and set a framework for European exchange. [10] Eurojust intends to assist cooperation at the judicial level between legal systems of the EU member states and with third states.

Offline or online, the EU is willing to follow its core principles and values regarding the rule of law and fundamental rights. It is difficult to distinguish between transparency, awareness-raising, empowerment of individuals and tackling cybercrime acts. [2] [11] To analyze the effectiveness of the EU's policies regarding cybercrime the improvements of the 2017 renewed CSS, institutional settings and cooperation between member states on EU level shall be identified. Progress was made in the adoption of measures by the member states to combat sexual abuse and exploitation of children and child pornography with the amendment of criminal codes, procedures and sectoral legislation, coordination of national actors was able to improve. Interpol's International Child Sexual Exploitation (ICSE) database for illegal images is constantly expanding. The cooperation of member states became closer with the implementation of the Directive on Attacks against information systems and 14 additional states ratified the Budapest Convention since 2013. The EC3 became the focal point in the fight against cybercrime in which staff and resources rose. In cooperation with the EU member states' law enforcement difficult cases were able to be solved more easily. The so called *No More Ransom* project of the EC3 was adopted to raise awareness and enabled citizens to decrypt their ransomed devices for free. Furthermore the cooperation between Eurojust and Europol improved since 2013. [18]

The CSS has so far not been effectively enough in increasing online accountability due to lack of publicly available and accurate data on registrants of domain names which creates opportunities for criminals to hide their activities. Further remaining gaps are mostly in the establishment of prevention programs, infrastructure and investment. The number of child sexual abuse images and number of traffickers in child pornography have increased (81%), thus, more effective measures are required. The EC3 is a good approach for effective cooperation, monitoring and investigations; still it lacks staff and resources to be effectively in high-profile cases. [18]

2.3. Cyber Defence Policy and Capabilities

The CSS 2013, the advanced version of 2017 and the Reflection Paper on the Future of European Defence acknowledge that the vulnerability of the supply of essential services as healthcare and water has risen due to the interconnectedness of the cyberspace. Furthermore the EU stresses the fact, that foreign governments outside of the EU abuse cyberspace for surveillance and manipulation. In order to tackle the unintended as well as intendent threats to the European cybersecurity the CSS focuses on detection, response and recovery. It seeks to improve the "synergies between civilian and military approaches in protecting critical cyber assets". [10] The CSS 2013 also gives priority to the information exchange between the EU and the member states as well as the risk assessment, awareness raising and the establishment of the cybersecurity. In addition, the industry and academia shall be fostered in order to develop and coordinate new solutions to reduce the cyber threats. One of the most important measures of the CSS 2013 is the use of the "network of NIS competent authorities […] to share information and support. This would enable preservation and/or restoration of affected networks and services." [10] Besides that, the EU

mentions that “it is predominantly the task of member states to deal with security challenges in cyberspace, this strategy proposes specific actions that can enhance the EU's overall performance.” [10] In order to tackle the threat of cyber-attacks as efficient as possible the EU aims to avoid duplications and strains to strengthen the international cooperation within the EU-US Working group as well as NATO, OECD, UN and further international organizations. The CSS also seeks to deter cyberattacks. Consequently, a foreign cyber-attack could lead to the invocation of the EU Solidarity Clause, Article 222 of the Treaty on the Functioning of the EU. [10]

The CSS 2017 refines the previous CSS and strengthens the deterrence approach. Thus, in the case of a cyber-attack the public authorities are supposed to response fast and effective in order to build confidence in the ability to avert a cyber-attack. A deterrence comprises a successful attribution, i.e. the detection of a cyber-attack as well as the assignment of it to the aggressor. Therefore, the CSS 2017 aims to improve the attribution of a cyber-attack with the implementation of IPv6, which shall allow an improved identification of a single user and raise the likelihood to detect the aggressor. The effectiveness of IPv6 is, however, doubtful, because despite of a wholesale adoption of IPv6 potential aggressor still would be able to use anonymous proxy servers or TOR browsers to obscure their attacks. Moreover, a cross-border cooperation within the EU as well as the establishment of an electronic platform to exchange information will accelerate the attribution. In order to tackle the fast-evolving cyber threats the CSS also claims the need for an efficiently functioning Computer Emergency Response Team. Therefore an EU Cyber Capacity Building Network will have to be established, which comprises the EEAS, member states‘ cyber authorities, EU agencies, Commission services, academia and civil society. Another aim of the EU is to strengthen the CSDP’s ability to tackle cyber threats within the framework of PESCO and the EDF. Apart from that, the CSS 2017 also refers to the Reflection Paper on the Future of European Defence. [19] The Reflection paper contains three possible kinds of defence integration between the member states. The first kind of integration comprises an exchange of information on cyber-threats and attacks, the second one aims at a stronger cooperation and the third one seeks a better coordination on cybersecurity within the member states. [20]

There are several challenges to the maintenance and development of European cyber security, which are mainly addressed by the CSS. The most important challenge of cyber-threat is the attribution of attacks. There are further challenges like the protection of less protected critical infrastructure on the municipal stage. These challenges shall not be outlined, as the CSS mainly concentrates on deterrence. An important condition for a credible deterrence is to detect and attribute the aggressor. Without an attribution the enforcement of laws or regulations would be unrealistic. [21] The attribution problem can be outlined in an attack against the Iranian nuclear enrichment facilities in Natanz, which has suffered the what is probably the most harmful cyber-attack by the malware Stuxnet. [22] At first the Iranian scientist assumed that the incident was an accident. After several weeks the accident was declared as a cyber-attack. By now it is not clear whether the USA or Israel was the aggressor. This example shows, how problematic a proper and fast attribution is. The detection of a cyber-attack takes averagely 150 – 200 days, the attribution itself can take months or even years. An exact attribution requires more information and time, than a less accurate attribution. The right for self defence according the UN Charta Article 51, however, demands an immediate reaction. Considering the long timeframe of the attribution the delayed retaliation measure could be seen as a new aggression. Otherwise a fast and less accurate attribution could lead to take measures against the wrong state, which could lead to a political escalation. [23] Hereby it is also noteworthy, that the complexity of attribution ease false flag attacks. [21] Thus, a credible deterrence requires a fast and proper attribution. Therefore the European decision to implement IPv6 is the right step to improve the ability to attribute, but it is also necessary to set up

– as the EU also intends – a platform, which fosters data exchange on cyber-threat incidents. This platform should seek to provide the actors with data mining techniques and statistical analysis. These elements could deliver further information about the aggressor, which raise the degree of certainty. Yet, the positive effects of an information exchange, which was prioritized by the CSS 2013, could be diminished by several problems. Firstly, if a member state shares its information about a cyber aggressor, other member states will also postulate further information about the way how data was collected and who received it. The receiving member state requires this accurate information in order to ensure an exact attribution, but it is very unlikely that the sharing member state will provide all these information. [21] Thus, the European member states do not receive all required information in order to establish an EU-wide security network as well as grant an effective attribution. [4] Secondly, a contextual understanding of the shared data is necessary. The gathered information is only useful, if the cyber intelligence experts of a member states are sufficient trained to interpret the information as well as the linked digital forensic traits and geo-political factors. Finally, it is very expensive to take part in the information gathering. It requires new hardware, software and training of new processes. [21] Considering the hard- and software‘s life cycle of two to three years, the public sector will always have to be always up to date in order to guarantee a successful attribution and deterrence. That means, that the current life cycle of public procured devices of five to ten years will have to be reduced. [24]

Unfortunately the EU neither stresses these problems nor suggests possible concrete solutions to it. That is why, some recommendations shall be proposed in the next section of this essay.

3. Recommendations for actions

Cyber resilience

The objectives of resilience should be defined more precisely: Is it 'just' about the ability to fend off attacks, endure and repair damage, or is there an additional need to build structures such as second strike capabilities or new forms of outer defense in order to already be able to reduce the occurrence of such attacks and damage? In this context, it would be useful for the Commission to devise a definition adapted to the real possibilities of action in form of an European White Paper on cyber resilience. With regard to the NIS Directive, which in principle goes in the ‘right’ direction, consideration should also be given to including digital SMEs and internet providers. This would mean that the definition of critical infrastructure would have to be revised. However, in view of the equally high vulnerability of smaller digital companies, they should also be required to provide security measures in the general interest. The certification of IT products should be legally binding, rather than voluntary, in order for the NIS Directive to be fully effective. In addition, a liability for hardware and software manufacturers should be considered. It should also be mentioned that the issues arising, such as the required protection profile and the scope of liability, should be discussed broadly and openly with all relevant stakeholders. The newly created certification and liability framework could put pressure on the world market by compelling non-EU manufacturers to implement European regulations in the context of market access. This in turn could lead to competitive advantages for European companies in a growing and sustainable industry. [11]

Cybercrime

Since cybercrime is crossing nations and effective law enforcement cannot be limited within state borders, the collaboration and cooperation between member states and the EU is essential to increase private and public safety “to make the EU's online environment the safest in the world.”

[10] To be highly effective in the reduction of cybercrime it is important to avoid institutional overlaps, focus on a clear distinction of resources and experts and ensure an appropriate investment in infrastructure and capacities. The EC3 shall remain the focal point in order to have a highly qualified contact institution for all member states in the field of prevention and investigation. The more trust of people and states in political processes of the EU are ensured, the more the system can be effective to combat cybercrime. The harmonization and qualification of tools, instruments and authorities is therefore essential. [13] To ensure the reduction of cybercrime in the EU, voluntary guidelines are not effective enough and it should be in the interest of all member states to cooperate and embed recommended guidelines into national law. To avoid monitoring incidents the cooperation of law enforcement regarding cybercrime reduction needs binding rules. Further needed is the increase in cooperation between Eurojust and Europol to identify challenges and possible solutions. [11] There have been proactive progresses in collaboration regarding the Budapest Convention. To make measures internationally more effective it would be progressive if additionally large countries as Russia, China or India would ratify the Convention. Supplementary the Budapest Convention, from 2001, needs to be modernized regarding today's needs. [25]

Cyber Defence Policy and Capabilities

The EU has to raise awareness for the problems linked to the attribution. The sharing of member states' experiences with the EU would be very helpful to identify cyber-attacks and to attribute them correctly. In the short term the EU could create incentives and financial support with the EDF in order to tackle the problems with the information sharing. [21] So, the task of the EDF could be expanded in order to support member states with a lower defence budget to afford the high expenses for hard- and software as well as the cyber-training program for intelligence staff. This would strengthen the cyber defence capability of every single member state and hence the defence capability of the EU. It would especially make it easier to gather information gathering and data analysis. Considering the importance of a comprehensive and profound information and data exchange, the EU should aim to build confidence between all member states' intelligence agencies and strengthen the interconnectivity of these agencies. In the long run it would be sensible to establish a well-equipped European center for cyber defence, which bundles all necessary competences and capabilities in order to fasten the attribution of broad cyberattacks and, in a second step, to avert them. Such a center would be especially auxiliary to defend small member states like the Baltics, which are not be able to defend themselves.

4. Conclusion

In summary, the European Commission, as part of its renewed CSS, has been fortunate enough to acknowledge that cybersecurity issues play an essential role in the security, freedom and prosperity of EU citizens in the 21st century. It is therefore to be welcomed when it is suggested to expand the public spending in education, training and cutting-edge research in order to be ready for the risks of the digital age. The expressed desire for increased European cooperation on cybercrime and cyber defence issues is urgently needed. On a positive note, the Commission recognizes that only a multidimensional approach involving business and civil society can ensure a sustainable balance between security and freedom. In a world that is becoming increasingly complicated, it is crucial for the future of Europe to speak with one voice on all crucial issues of internal and external security while making the most of the (digital) single market.

At the same time, however, this paper shows that the EU is still a long way from a system of standardized procedures, automatic data reconciliation and equivalent cyber resilience rules across

all member states. The national governments are still firmly in the grip of action in the central areas of foreign and security policy, on the one hand, and domestic and justice policy on the other. There is a risk that larger and economically more potent member states will work alone and strengthen their cyber resilience and cyber defence capabilities, while smaller and weaker member states lag behind. It must be remembered that the EU has a high degree of interdependence due to its single market and open borders, so risk assessment is never just about how well one's own country is set up, but about keeping the EU as a whole in mind. As a result, the EU is only as resilient as its least resilient member state.

In order for the Commission's efforts to be fruitful, the European treaties would need to be amended so that the ordinary legislative procedure is applied to CFSP and CSDP. Finally, the EU would be more than just a coordinating layer of diverse national regulations, and could indeed provide for a significantly increased level of cyber resilience, a more effective fight against cybercrime and a common cyber defence policy with substance.

5. References

[1] BARTH, J. D. / SCHLEGELMILCH, W.: Cyber Democracy: The Future of Democracy?, in: Carayannis, E. G./ Campbell, D. F. J./ Efthymiopoulos, M. P. (ed.), Cyber- Development, Cyber-Democracy and Cyber-Defence. Challenges, Opportunities and Implications for Theory, Policy and Practice, Springer, New York/ Heidelberg/ Dordrecht/ London, 2014, p. 195-206.

[2] MITTERLEHNER, B.: Cyber-Democracy and Cybercrime: Two Sides of the Same Coin, in: Carayannis, E. G./ Campbell, D. F. J./ Efthymiopoulos, M. P. (ed.), Cyber-Development, Cyber-Democracy and Cyber-Defence. Challenges, Opportunities and Implications for Theory, Policy and Practice. Springer, New York/ Heidelberg/ Dordrecht/ London, 2014, p. 207-230.

[3] TAMMINGA, O.: Zum Umgang mit hybriden Bedrohungen. Auf dem Weg zu einer nationalen Resilienzstrategie, SWP-Aktuell 2015/A 92, November 2015, available online: https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2015A92_tga.pdf, 11/2015, p. 2f. (Accessed on January 14, 2018).

[4] BENDIEK, A.: Das neue >>Europa der Sicherheit<<. Elemente für ein europäisches Weißbuch zur Sicherheit und Verteidigung, in: SWP-Aktuell 2017/A 37, Berlin 2017, available online: https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2017A37_bdk.pdf, p. 5. (Accessed on February 2, 2018).

[5] EUROPEAN COMMISSION (2017): Proposal for a regulation – COM(2017) 477/947932

[6] EUROPEAN UNION: Regulation (EU) 2013/526

[7] EUROPEAN UNION: Directive (EU) 2016/1148

[8] EUROPEAN COMMISSION: Cybersecurity - EU Agency and Certification Framework, available online: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-eu-cybersecurity-agency-and-eu-framework-cybersecurity-certification, 2017. (Accessed on January 18, 2018).

[9] EUROPEAN COMMISSION: Commission Recommendation (EU) 2017/1584

[10] EUROPEAN COMMISSION: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

[11] BENDIEK, A./ BOSSONG, R./ SCHULZE, M.: Die erneuerte Strategie der EU zur Cybersicherheit. Halbherziger Fortschritt angesichts weitreichender Herausforderungen. SWP-Aktuell 2017/A 72, October 2017, available online: https://www.swp-berlin.org/fileadmin/contents/products/aktuell/2017A72_bdk_etal.pdf, 2017, p. 2-4; 4f. (Accessed on January 08, 2018).

[12] COUNCIL OF THE EUROPEAN UNION: Draft Council conclusions on the Joint Communication to the EP and the Council: Resilience, Deterrence and defence: Building strong cybersecurity for the EU, 14435/17, available online: http://www.consilium.europa.eu/media/31666/st14435en17.pdf, 2017. (Accessed on January 21, 2018).

[13] PETRATOS, P.: Cybersecurity in Europe: Cooperation and Investment, in: Carayannis, E. G./ Campbell, D. F. J./ Efthymiopoulos, M. P. (ed.), Cyber-Development, Cyber-Democracy and Cyber-Defence. Challenges, Opportunities and Implications for Theory, Policy and Practice, Springer, New York/ Heidelberg/ Dordrecht/ London, 2014, p. 279-302.

[14] CSIS- CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES: Net losses estimating the global cost of Cybercrime. Economic impact of cybercrime II, Report, available online: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/McAfee%20and%20CSIS%20-%20Econ%20Cybercrime.pdf, 2014, p. 20. (Accessed on January 09, 2018).

[15] EUROPOL: The relentless growth of cybercrime, available online: https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime, 2016. (Accessed on January 09, 2018).

[16] BENDIEK, A.: Europäische Cybersicherheitspolitik. SWP-Studie, available online: https://www.swp-berlin.org/fileadmin/contents/products/studien/2012_S15_bdk.pdf, Berlin, 2012. (Accessed on January 12, 2018).

[17] EUROPOL IOCTA: Internet Organized Crime Threat Assessment, available online: www.europol.europa.eu, 2016, p. 7f.; 40. (Accessed on February 02, 2018).

[18] EUROPEAN COMMISSION: Commission Staff Working Document. Assessment of the EU 2013 Cybersecurity Strategy, available online: https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF, 2017, p. 36-41. (Accessed on February 01, 2018).

[19] EUROPEAN COMMISSION: Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 2017, p. 12-14.

[20] EUROPEAN COMMISSION: Reflection Paper on the Future of European Defence, available online:https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf, Brussels, 2017, p.12-14. (Accessed on February 01, 2018).

[21] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE: Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks, Pihelgas M. (ed.), available online: https://ccdcoe.org/sites/default/files/multimedia/pdf/False-flag%20and%20no-flag%20-%2020052015.pdf, Tallinn, 2015, p. 8; 21. (Accessed on February 01, 2018).

[22] TABANSKY, L.: Cyber Security Challenges: The Israeli Water Sector Example, in: Clark, M. R./ Hakim, S. (ed.), Cyber-Physical Security. Protecting Critical Infrastructure at the State and Local Level, Philadelphia, 2017, p. 205-221.

[23] REINHOLD, T. / SCHULZE, M.: Digitale Gegenangriffe. Eine Analyse der technischen und politischen Implikationen von „hack backs“, in: SWP, available online: https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf, Hamburg, 2017, p. 8f. (Accessed on February 02, 2018).

[24] MATTHEWS, E. D./ ARATA III, H. J./ HALE, B. L.: Cyber Situational Awareness, in: Connolly, C. (ed.), The Cyber Defence Review. A dynamic multidisciplinary dialogue, New York, 2016, p. 35-48.

[25] CHATHAM HOUSE: Building a Stronger International Legal Framework on Cybercrime https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime, 2017. (Accessed on February 01, 2018).

eGovernment IV

ON E-GOVERNANCE DEVELOPMENT OPPORTUNITIES IN THE REPUBLIC OF MOLDOVA

Mihai Grecu[1], Igor Cojocaru[2] and Ion Coşuleanu[3]

DOI: 10.24989/ocg.v331.27

Abstract

The process of e-Governance building in the Republic of Moldova, amplified with the adoption of the e-Transformation governmental program, highlighted the issues that require a proper approach to local conditions and specificities.

A specific feature of Moldovan society is that the country's population is mostly rural. In rural areas, the sensitivity to new services and the affordability of ICT tools are lower. Another feature is that the administrative structure at the local level is very fragmented; the administrations manage small budgets that cannot cover the needs of implementing e-Governance solutions.

In general, the capacity to finance ICT projects in the public sector is below the need. At the same time, some trends and indicators regarding the level of e-Governance development in the Republic of Moldova: literacy level, ICT skills, access to the Internet, use of mobile telephony, use of electronic services, etc. shows that there is significant potential to explore new opportunities, in particular, based on innovation and involvement of different social partners to support efforts to build e-Governance.

The article addresses the issue of identifying new opportunities for e-Governance solutions in the context of economic and social disparities present in the Republic of Moldova. The opportunities are based on more active involvement of social stakeholders, the use of more affordable new technologies, and the adoption of policies aimed at optimizing the use of available resources.

1. Introduction

E-Governance is today perhaps the most popular topic and an unprecedented challenge to public administration reform in a broad context of building the information society. The e-Governance model - a citizen-centered public service system that replaces the traditional service service with a new one based on the Internet and information technology, provides a modern approach to public services that ensure transparent and unified communication between government institutions to enhance the potential public services and governance in general. E-Governance initiatives are evolving to keep pace with the ever-changing dynamics of increasingly advanced technology solutions and respond to the increasing demand of citizens for higher quality public services.

Originally developed in countries with strong economic and technological potential, concepts and models of e-Governance, taken over by countries in transition, did not lead to expected results [7]. The explanation is that the processes in a country's public administration are part of a system that is too complex in terms of economic, social, cultural, etc. which is the country's specificity - an

[1] Information Society Development Institute, Chişinău, Moldova, mihai.grecu@idsi.md
[2] Information Society Development Institute, , igor.cojocaru@idsi.md
[3] Information Society Development Institute, ion.cosuleanu@idsi.md

unrepeatable one that must be carefully considered when it comes to identifying e-Governance solutions.

The e-Governance concept evolves continuously as more and more information and experience accumulates in its development. The aim is to bring added value to public services. To this end, government is gradually giving up its traditional, simplistic and mechanistic way of delivering services and becomes a flexible platform, oriented to citizen and its interests, which offer services of great complexity and value [4]. Such a transformation does not lack the public administration of institutional powers and abilities, becoming more proactive, with more possibilities to focus on the efficient management of public activities and relations with citizens, many activities being taken up by social actors outside the public administration who apply specialized infrastructures and expertise.

E-Governance initiatives in Moldova added value to the governmental act [5], but they also highlighted some of the issues whose solving is a key issue for the further development of the e-Governance system. In the authors' opinion, they specifically refer to the following aspects:

- Identifying a conceptual model of e-Governance adequate to the conditions and realities of the Republic of Moldova;

- building public data infrastructures to ensure a common and coherent information space to support the homogeneous development of e-services at all levels of government;

- A broad involvement of several social actors in intensifying efforts to develop e-Governance in the Republic of Moldova.

2. Background

Moldova has made some successes in e-Governance: a high level of EGDI (E-Government Development Index), in particular, of online services (Table 1), on a high-performance telecom infrastructure (Figure 1), capable of ensuring the provision of electronic public services across the country.

Rank	Country	e-Government Development Index	Online Service Index	Telecomm Infrastructure	Human Capital
35	Russian Fed.	0,7215	0,7319	0,6091	0,8234
36	Poland	0,7211	0,7029	0,5857	0,8747
46	Hungary	0,6745	0,6304	0,5615	0,8317
49	Belarus	0,6625	0,4855	0,6304	0,8716
50	Czech Republic	0,6454	0,4783	0,5952	0,8627
52	Bulgaria	0,6376	0,5652	0,5602	0,7875
62	Ukraine	0,6076	0,5870	0,3968	0,8390
65	**R. of Moldova**	**0,5994**	**0,5942**	**0,4850**	**0,7191**
67	Slovakia	0,5915	0,4420	0,5504	0,7822
75	Romania	0,5611	0,4565	0,4533	0,7736
	Eastern Europe	*0,6422*	*0,5674*	*0,5428*	*0,8166*
	Europe	*0,7241*	*0,6926*	*0,6438*	*0,6897*

Table 1: E-Government Development Index in Eastern Europe countries, 2016 [12]

More and more electronic public services for citizens and businesses have been developed and are being used: information services, transactional services - electronic payments, etc., all of which have created prerequisites for a deeper and multilateral approach to e-Governance. The Strategic Programme for Technologic Modernization of Governance (e-Transformation) [14], adopted in 2011, boosted the development of e-Governance and created premises for profound transformations and modernization of public services.

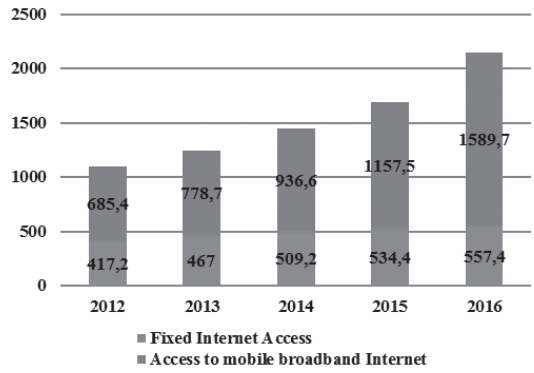

Figure 1: Broadband Internet access, thousands of users. The National Regulatory Agency for Source: Electronic Communications and Information Technology (ANRCETI), http://en.anrceti.md
Note: Moldova population: 3,551 thousand .Source: www.statistica.md

Moldova is a developing country, and a characteristic for such countries [8] it is that IT public budgets are neither stable nor appropriate to needs, and usually public sector IT projects are funded by donors. In many cases, their implementation is not preceded by studies of the real situation in the country, project sustainability is not ensured - once external funding ceases, projects are no longer supported, and there is often no policy coordination in IT projects. It happens that different projects deal with the computerization of the same processes. Efforts focus mainly on computerization of traditional processes, not on transforming business processes and streamlining governance services.

As confirmation in our case, the most important project in the area of eGovernance over the last 7 years - the e-Government Transformation Program in Moldova has been supported by the World Bank's International Development Association (IDA) in the amount of 20 million USD. However, budget allocations for IT in the public sector are well below the level needed. In 2016, expenditures for computerization of public administration, defense and compulsory insurance amounted 260 million lei or about 15 million USD, which represents 0.22% of the GDP of the country - 6.75 billion USD.

Also, a recent report by the Court of Auditors [9] on the implementation of the e-Transformation of Governance Project reveals a number of shortcomings including:

- Lack of effective tools for coordinating activities,
- Ambiguities and inconsistencies in the functioning of the implementing bodies;
- Sporadic and uncoordinated use of electronic services;
- Exhaustive evaluation of necessary resources;

- Non-transparency and inefficiency in the digitization of services;
- Digitizing front-office processes, while back-office processes are still out of digitization;
- Incapacity of public entities to ensure the sustainability of e-services implemented.

The approaches to implementation of e-Governance solutions so far have been made mainly at the central level of public administration [5], [9]. At the same time, most of the public services remained outside digitization, because at local level there is neither the economic potential nor the necessary expertise.

There is a large discrepancy between the level of ICT use in the capital, Chisinau municipality, compared to the rest of the country (Figure 2, Figure 3). Basically, the bulk of investments in computer-related activities across the country are carried out in Chisinau. This is happening on the background of a rural majority of the country's population - 57%.

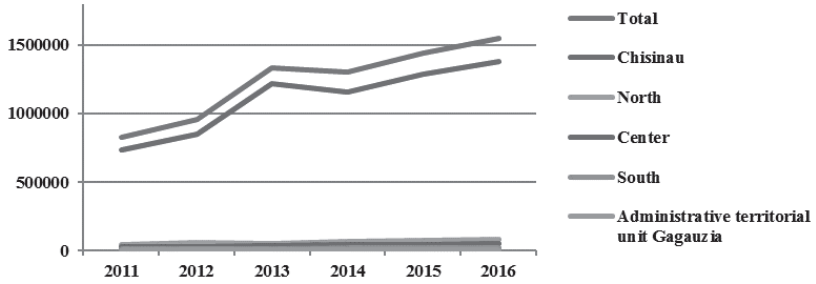

Figure 2: Expenditure of legal entities for information technology, thousands lei, Source: NBS www.statistica.md

The income of the majority of the population is modest (Figure 3) and therefore ICT accessibility is low, making it difficult to uptake e-Governance services and hence increases the risk that investment in e-Governance projects will be below expectations in efficiency and effectiveness. The difference between Chisinau and the rest of the country amplifies this phenomenon and puts very difficult additional tasks ahead of e-Governance.

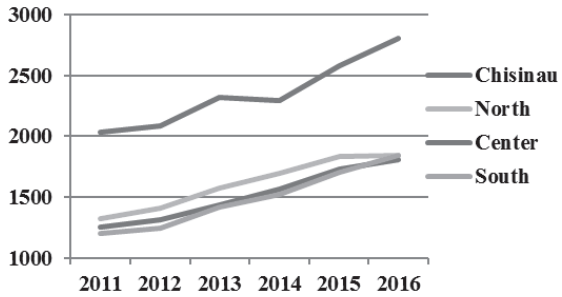

Figure 3: Monthly average earnings per person, lei, Source: NBS www.statistica.md.

Electronic services in Moldova's e-Governance system are, in fact, services provided by agencies and departments that are in line with the traditional mode of delivery [5], [9]. Their level of interoperability is low, being largely services that represent service requests:

- Request for the release of the criminal record to individuals;
- Free access to data from the real estate register;
- Request for the issue, extension and reperfusion of activity licenses;
- Verification of the personal identification code;
- Request to issue the duplicate birth certificate, etc. (servicii.gov.md).

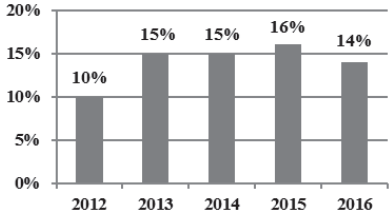

Figure 4: Access to the Government portal, % of population, Source: eGov Center, www.egov.md.

A service is usually provided through the site of the institution responsible for this service (Figure 4, Figure 5), but not in a common framework where several services from different agencies interact. For example, it can be applied online to obtain a criminal record, but the applicant will take the document from the issuing agency and will personally present it to the institution that requested it.

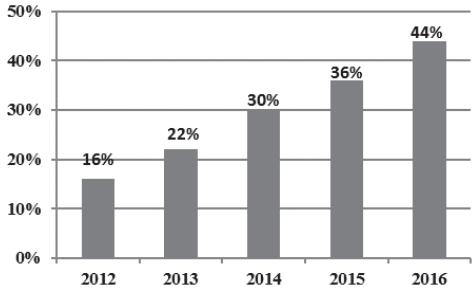

Figure 5: Accessing government agencies sites,% of population, Source: eGov Center. www.egov.md.

The degree of maturity of service models is still low. There are some interactive services as well as transactional services initiatives. We need to mention here the governmental electronic signature service - Msign, the national service for authentication and access to electronic public services - Mpass, Public e-Reporting Service - e-Reporting, MPay - electronic payment of public services. The service integration phase is to be carried out at further stages by implementing advanced interoperability models.

Local authorities, especially those in rural areas, face major difficulties in implementing e-Governance. For the most part, they lack the capacity to deploy independent, high-complexity and high-performance electronic services [1], [2], [8]. It is known, however, that citizens and business most often interact with local government [1], [2], [13]. Therefore, identifying solutions for e-Governance at local level is a matter of the greatest importance, and, in order for these administrations to be able to implement and operate efficiently e-Governance services, there must be ensured interoperability on multiple levels between services, data, processes in the central administration, and all local governments so that synergy results in efficiency.

3. The need for an appropriate reference model of e-Governance

E-Governance is today a vital condition for public administrations to be able to deliver efficient and cost-effective services in response to the growing demands of citizens and businesses on their promptness, complexity and quality. E-Governance has the role of bringing substantial added value to public services.

Efforts that have been made in field of computerization of public sector activities and ICT-based modernization have resulted in the informational solutions that have been implemented in the public sector largely based on old, bureaucratic, strongly segmented governance. This mode does not serve government because it does not improve communication between different government entities. It does not fully serve the needs of citizens and business, but rather, it can lead to a low level of absorption and use of the means of information technology, and inefficiency in the spending of public money [2].

The computerization of public services and internal public administration activities mainly referred to the technical aspects and did not generate essential changes in business processes and workflows, or structural changes in the activity of governmental institutions. The analysis of the e-Governance implementation activities [9] reveals weaknesses of the institutional framework that have influenced the achievement of the stated objectives, ambiguities and inconsistencies in the management's assurance. Also, mechanisms for monitoring and measuring the achievement of project objectives have not been implemented to the necessary extent.

To avoid this dispersion and to make efforts to develop e-Governance in Moldova more efficient, it is imperative to adopt a reference model of e-Governance, feasible and appropriate to local social and economic conditions and to ensure the sustainability of the process to full maturity.

A basic principle of the e-Governance reference model should be to ensure the interoperability of governance components throughout the public administration information space and, above all, semantic interoperability as a decisive factor in ensuring the consistency of public information. The reference model for the e-Governance system in Moldova must present a logical structure that defines the stages and levels of maturity in the evolution of the system as well as a methodology to measure and monitor the development process of the system.

4. Common data infrastructure

A major challenge of national policy on modernizing public services within the e-Governance system is access to information and data. Solutions in this sense will have to respond to the need to save time, money and other resources necessary for efficient use of data, and these solutions will need to ensure interoperability of data in order to provide services.

The volume and diversity of public data is steadily increasing. Heterogeneous data sets must be able to be accessed and used in highly complex integrated services. This requires identifying models and mechanisms to ensure the coherence and interoperability of data in a single information space in the public sector in strict accordance with European principles, recommendations and practices [3] eliminating redundancy, ensuring availability, openness, transparency in maximum safety.

E-Governance initiatives aim at an increased level of communication in a wide variety of situations in the areas of public administration. In order to ensure the integration of government services at government level (whole government approach), good coordination between users and information providers is required so that information and knowledge from different sectors of government can be used in a common context. Developing e-Governance policies requires an integrated and comprehensive approach that takes into account the specificities of each public domain of activity.

The availability, quality, organization, accessibility and sharing of government information needed to achieve the objectives set in e-Governance initiatives requires the adoption of measures on the sharing, access and use of interoperable government data and services. They should aim at setting up a government-wide information infrastructure to support policies and activities on public services. Such infrastructure will use information infrastructures within different public authorities with common rules, actions and measures at national level in a unitary context of the whole government.

The Common Data Infrastructure will allow for the creation of opportunities for the development of e-services across the entire public information area for all stakeholders.

5. Wide involvement of social stakeholders in building e-Governance

The real conditions of developing and implementing e-Governance solutions in Moldova present a multitude of impediments and risks. The government's ability to ensure process feasibility is significantly limited. The process can not continue indefinitely, being financed almost entirely by outside financiers. There is a need for social cohesion around a common cause of e-Governance of a large number of stakeholders in society.

The population of Moldova is very rural - about 57%, while a large part of the population lives in small towns. In total, they account for about ¾ of the entire population, in an environment that is not conducive to the development and absorption of high-performance e-Governance.

The issue of implementing eGovernance is a societal one, and solutions have to be identified through broad society participation. Experience and good practice in this respect show that the participation of the various social actors, first of all, of the private sector [10], [13], is crucial for ensuring the sustainability of the development and implementation of e-Governance services. In order to encourage and motivate local ICT businesses, but also to fill huge gaps in the capacity (Figure 3) to provide e-Governance solutions with the necessary resources, social eGovernance collaboration policies are required as many stakeholders as possible. Governance can and must share resources and services with society so that synergy of collaboration produces results expressed in quality services, close to the needs of the citizen, accessible to local business and in line with trends in the field.

The Information and Communication Technology sector is experiencing rapid development in recent years, constituting about 8% of the Gross Domestic Product of the Republic of Moldova,

according to the ministry's data (www.mtic.gov.md). IT service exports have increased 15 times over the last 5 years.

The benefits of multi-stakeholder participation in the e-Governance implementation process are evidenced by international practice [10], [11], [13], as well as by some successful local practice initiatives, such as the mPay electronic payment service (https: // mpay.gov.md/), which was realized and is provided in collaboration with institutions from the banking system, the mobile signature service (http://egov.md/ro/projects/semnatura-mobila), which is a collaboration of governance with mobile providers, and so on.

The problem is to identify effective ways and solutions that will contribute to mobilizing the potential of the IT and related sectors in the efforts to develop and implement e-Governance services in the spirit of best practices in the European and international space [1], [2], [10], [11].

6. Conclusions and recommendations

e-Governance has had a significant development in the Republic of Moldova and has achieved notable performances recorded in national and international reports.

The development of the e-Governance system in Moldova is currently facing a number of challenges. They depend, on the one hand, on the modest economic and social potential of public administration, especially at local level, to bear the costs of development and, on the other hand, on the organization and functioning of the public administration which, at the current time is not ready for profound transformations being heavily segmented from a structural and functional point of view.

Activities aimed at implementing e-Governance services have not yet gone beyond the departmental framework and have not ensured the coherence and interoperability needed to develop integrated, complex, high performance services.

Intensifying and accelerating the implementation of e-Governance in Moldova depends on how they will be identified and new opportunities will be created.

The opportunities lie in a new vision and system approach of activities for the development of the e-Governance system at all levels of public administration.

In this respect, it is necessary to adopt a conceptual reference model of e-Governance in the Republic of Moldova that will serve as a conceptual benchmark and methodological guide for the e-Governance development actions on the whole spectrum of activities in the public sector throughout the development period system.

Particular attention should be paid to the problem of establishing a common data infrastructure in public administration that ensures information coherence and interoperability between all departmental data infrastructures and enables the development of integrated services at all administrative levels.

Governance is today unable to cope with all the tasks that stand before it on the development of e-Governance solutions, and in this sense it needs to work more closely with the business community and civil society to provide citizens with services high performance. Governance with social

partners can ensure the sustainability of e-Governance, and stakeholders in society can take up some of the burden of public services, thereby creating real development opportunities.

Governance can and must share resources and services with society so that synergy of collaboration produces results expressed in quality services, close to the needs of the citizen, accessible to local business and in line with trends in the field.

7. References

[1] ICT for Local Government. Handbook. E-Governance Academy. 2007. http://ega.ee/wp-content/uploads/2015/02/project_ICT_for_Local_Government.pdf

[2] RAHMAN, Hakikur, Framework of E-governance at the Local Government Level. In: Comparative E-Government. 2010. http://www.springer.com/gp/book/9781441965356

[3] Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017. https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration

[4] MULDER, H., KONTAKOS I., Rethinking the Public Spending on ICT projects. https://www.standishgroup.com/sample_research_files/Dutch4.pdf

[5] GRECU, M., COSTAȘ I., A. Reaboi. E-Government Services in Moldova: Value and Opportunities. Proceedings of the Central and Eastern European e|Dem and e|Gov Days 2017, Budapes.

[6] Governance eTransformation Project - Financial Statements 2012. http://egov.md/ro /transparency/ reports/audit-proiect-etransformarea-guvernarii-anul-2012.

[7] HEEKS, Richard, e-Government Benefits And Costs: Why e-Gov Raises Not Lowers Your Taxes. https://ict4dblog.wordpress.com/2011/09/29/e-government-benefits-and-costs-why-e-gov-raises-not-lowers-your-taxes/.

[8] PARDO, Theresa A., NAM Taewoo and BURKE G. Brian, E-Government Interoperability: Interaction of Policy, Management, and Technology Dimensions. Social Science Computer Review 2012 30: 7 originally published online 12 January 2011.

[9] Performance / IT Audit Report "What are the progress and impediments / risks in the implementation of the e-Government Transformation Project?" (romanian). http://lex.justice.md/index.php?action=view&view= doc&lang=1&id=373768.

[10] VASSIL, Kristjan, Estonian e-Government Ecosystem: Foundation, Applications, Outcomes. 2015. http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf.

[11] eGovernment Benchmark 2017. Taking stock of user-centric design and delivery of digital public services in Europe. https://www.capgemini.com/consulting/wp-content/uploads/sites/30/2017/11/2017-egovernment-benchmark-insight1.pdf.

[12] United Nations e-Government Survey 2016. E-Government in Support of Sustainable Development. http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf.

[13] Public-Private Partnerships in e-Government: Knowledge Map. https://www.infodev.org/infodev-files/resource/InfodevDocuments_821.pdf.

[14] Strategic Programme for Technological Modernization of Governance (e-Transformation) http://lex.justice.md/viewdoc.php?action=view&view=doc&id=340301.

A self-reflection of municipal IT professionals in small Romanian city administrations

Nicolae Urs[1]

DOI: 10.24989/ocg.v331.28

Abstract
E-government usually studies focus on outcomes or user opinion. Our attempt is to see this also from the point of view of IT professionals that work in public institutions. Big cities will always be on the forefront of using new technologies in their day-to-day work and, because of that, they are usually the subject of researchers wanting to study this field. But most Romanians live in small cities, towns and villages. We are also interested in the pace of e-government development in these municipalities.

After the 2017 study that focused on big Romanian cities, this year we follow up with a more comprehensive research, which aims to find out how e-government is implemented in small urban municipalities in Romania. Our research aims to learn how successful the implementation of e-government services in Romanian local government is in the eyes of those tasked with rolling out these services. E-government is no longer a new development in the public institutions' continuing search for better service. The interaction between citizens and companies, as well as the government, are constantly evolving, and new ways of doing things are regularly tested and adopted or discarded.

Keywords: *e-government, local government, public servants' view, Romania*

1. Introduction

Any digital interaction requires at least two parties, which, in the case of digital government, are usually citizens or companies (accessing services offered online) and public servants or public institutions (as the providers of said services). When trying to find out the success of one e-government project or another, most researchers turn, understandably, to the beneficiaries. Citizens' opinions on the level of government digital development feature prominently in a fair number of studies. The voices of public servants seem to be less heard, even if they are also using the services in their day-to-day work. Among the public employees, ICTs professionals are instrumental in designing, implementing, upgrading, and troubleshooting the digital offerings of the public institutions. Following the 2017 research, which focused on Romanian big cities, this time we are taking a closer look at city halls from small cities and towns and their ICTs specialists and analyzing their opinions on e-government development in Romania, both in their institutions and at the national level.

Like any important concept, e-government has an increasing number of definitions. Back in the day, when e-government was a new topic, those definitions dealt mainly with technological aspects and insisted on the process (web usage, the role of the internet infrastructure) [7] [9]. After the novelty wore out, researchers began looking into the perceived benefits of e-government, focusing their

[1] College of Political, Administrative and Communication Scciences, BBU, Cluj-Napoca, 85 Minerilor Street, Cluj-Napoca, urs@fspac.ro

characterizations on the improvements it could bring for the public institutions and in their relationships with the other actors [6], and how this new innovative way of doing things is benefitting citizens, companies or other public institutions [11]. What all these definitions have in common is an undercurrent of optimism about the benefits that the increasing sophistication of the digital services offered by the government, both local and central, can bring to society at large. Those benefits include increasing the productivity of public servants with the help of new technologies, increased transparency and accountability, better services offered to ”clients” (in the parlance of New Public Management proponents), and cost reductions, spurred by the increased automatization of processes inside institutions [8] [12].

This sunny outlook is dimmed a little nowadays, with some researchers pointing out that the hyped revolution in governance did not come to pass. Big differences between the expected and actual results made some experts to critique the technological determinism undertone that permeates this study field and to discount almost entirely any influence of ICTs on public institutions [13]. Even if they do not go that far, a number of studies point to the complications e-government projects encountered when moving from the drawing board to real life [14] [16]. A lot of these obstacles are embodied not by technological hurdles, but by the way people tasked with implementing these changes chose to treat the transformations that the increasing digitalization of public services brings (on a spectrum that stretches from enthusiastically embracing these changes to fiercely opposing them). Human capital in general is largely seen as essential for the success of digital projects and every effort should be made to increase the digital literacy of citizens so as to be able to understand and use the new services [3]; a higher level of digital knowledge also helps people in their day to day lives (online shopping, internet banking, on-demand media, online education are just some of the services that would be impossible without the last technological revolution and equally impossible to benefit from without at least basic digital skills).

For digitalization of government to work, the computerization of the public institutions (installing the technological infrastructure and creating or buying the necessary software) is not enough. The trickiest problem e-government projects usually encounter is convincing the public servants that this transformation is for the better, not only for citizens, but for the institution and for them as well [5]. The few studies on the attitudes of IT professionals from government institutions regarding e-government projects show that management support, interoperability and digital skills are seen as the main obstacles encountered in the quest to digitalize services [1].

If we look at e-government success stories throughout the world, countries that advance rapidly in this field are usually those that implement a well thought-out national strategy [2] [14], with as little political horse-trading on this topic as possible; such a national strategy usually takes much more than the typical 4 years of a ministerial term.

Electronic government development is mainly measured at country level. This preference stems partially from the type of organizations that have the knowledge and resources to do such studies and that are mostly international bodies of one kind or another – United Nations, The European Union, The Organization for Economic Co-operation and Development. These rankings provide a very good general overview, but, inevitably, lack the granularity to show differences between regions or municipalities inside countries. These differences matter, especially in countries such as Romania where the drive to modernize government and implement online services is not mainly a centralized effort, but a patchwork of local movements, each with its somewhat different characteristics.

Citizens are more interested in what happens inside their community because those developments have a direct effect on their well-being. The relationships between citizens, NGOs and companies, on the one hand, and local government institutions, on the other, are essential in making a community work. As such, studies that focus on local e-government or the way municipalities adapt to the changing technological and societal environment have started to become more common in the last 15 years [4] [10] [15].

2. The Situation in Romania

Romania offers a mixed bag in term of e-government successes. The first coherent national strategy on e-government development was published in 2008. Afterwards, the subsequent strategies were driven by the requirements of the European Commission and the targets Romania agreed to inside the Digital Agenda and the Europe 2020 strategies. However lofty the ideals espoused in those documents, in reality a centralized effort to implement the required tools, so that the different particular IT solutions adopted by Romanian public institutions could interconnect, was almost non-existent from 2008 onwards. There are some successful national initiatives (the public procurement platform, a payment platform for public institutions), but even those are not properly integrated into a national system.

Partly because of the slowness in developing digital government at the national level, many local government institutions developed their own bespoke solutions that, inevitably, could not be seamlessly integrated because of lack of shared standards and compatible infrastructure. Even inside local public institutions, there are seldom standards in place that require intra-institutional compatibility (for example rules demanding that the software bought by one department should follow a set of requirements so as to be possible to interconnect it with software already in place in other departments).

Romania is constantly ranked at the bottom of various classifications related to electronic government in Europe, in spite of a well-developed ICT sector and available European funds specifically allocated to digital government development. This image is a coarse one, and can hide very different levels of sophistication regarding the online services offered to citizens and companies by the different municipalities in Romania. In this regard, it is no surprise that big cities fare better. Their public institutions (mainly the city halls, because most of the services offered by the local governments are provided by city halls) have gradually increased the number and quality of online services delivered to citizens and companies. They are not on par with digital champions such as Barcelona, New York or Singapore, but they are steadily (although slower than a Romanian would like) moving in the right direction [15].

But not all Romanians live in big cities. More than 43% of people in Romania live in rural areas (among the highest proportion in the European Union). Even in the case of urban dwellers, only a little over half of Romanians live in cities bigger than 100,000 inhabitants. We were interested to see how e-government is perceived in small cities and towns that usually do not have the resources, know-how and trained workforce that bigger cities enjoy. We were interested in the inside view of public servants and not in the opinion of citizens this time, and for this we chose to ask the ICTs professionals in city halls in these towns their views on e-government progress, both inside their institutions and in Romania as a whole.

3. Methodology

We sent questionnaires (both online and by mail) to towns and cities in Romania with a population of under 40,000. The survey was aimed at the heads of IT departments (whatever they were called) in their city halls and, if no such department existed, the person responsible with answering citizens' questions was asked to respond to our queries. In some cases we talked on the phone with the responsible public servant to clarify some of their answers.

There are 263 towns and cities in Romania that fit that profile. For this study, we selected just the city halls that had a functional IT department (with at least 1 person working there at the moment of filling in the questionnaire). From the 125 responses we collected, 54 had no IT department in their institutions, and 11 more had some positions in their organizational chart, but they were not filled. After pruning some incomplete answers, we were left with 56 usable responses.

The towns and cities varied in size from 1,684 inhabitants to 38,970 and all regions of the country are represented in this sample. Data were cleaned with Google Refine and analyzed with the help of Microsoft Excel and Tableau Desktop.

In the 56 city halls that constitute our study population, most had only one IT specialist in their institution. In just 12 cases their IT unit consisted of two or more (just 2 instances) people.

We started our research with 4 hypotheses:

1. Romanian public institutions (in our case, City Halls) experience difficulties in filling IT positions;

2. Management support and internal reorganization of the institution are seen by the IT professionals as very important in e-government development;

3. The main obstacles in e-government development are lack of interinstitutional interoperability and the differences between pay in private versus public organizations;

4. Public pressure is an important factor in implementing electronic government.

But first, some general findings that became apparent after analyzing the responses we got. The problems faced by public institutions in small cities are somewhat different from those encountered by those in bigger cities in Romania.

4. Findings

To gauge the stage of their local electronic government, we asked them to tell us the online services they provide and their usage count. The most numerous online services present on their websites were, in order: paying taxes online (34 of them said they have such a system but only 19 were able to give us any user numbers); paying fines online (32 cities offer this service, but only 18 had any hard numbers) and filing a complaint online (with 13 institutions providing this option and 12 of them giving us statistics).

Regarding paying taxes online, which is seen by many as the most sought-after online service, the numbers show that a small percentage of citizens take advantage of this even when it is available:

City Hall	% of population paying taxes online
Roznov	1.94
Câmpia Turzii	1.59
Târgu Neamț	1.38
Boldești-Scăeni	1.22
Pantelimon	1.12
Reghin	0.75
Câmpulung	0.66
Gura Humorului	0.49
Vălenii de Munte	0.46

Table 1: Percentage of population paying taxes online

In their evaluation of the current state of government digitalization, 11 respondents think that the national level is lower than the local level, 10 think the opposite, while the remaining 35 consider that both the national and their own city are at about the same level of development. This contrasts with the results from last 2017 (which looked at the big cities in Romania), where the IT professionals who responded were much prouder of the achievements of their own institution compared to the perceived national level.

We asked the respondents if they had any previous work experience in a private IT company before coming into a public administration organization. Of the 56 usable answers, we found out that only 10 of them had worked in a private organization. Their marks on the level of electronic government development, both in their town, and in Romania as a whole, hovered around 2.65-2.70 out of 5, irrespective of their working experience. We were also a little surprised to find out that there are relatively few young people responsible for taking care of the technological infrastructure of the responding city halls: 55 shared their age, and only 8 were under 35 (only one under 30).

A pleasant surprise was the big increase in the number of agreements for data exchange between the city halls and other public institutions. More than 50% have such arrangements, and 14 out of those share data with more than one institution. The champion here is again the National Agency for Fiscal Administration (NAFA), but the field is increasingly crowded, with links between public organizations being created at a rapid pace. We must keep in mind that we are talking about small cities and towns that, presumably, have less interest and resources to forge such ties.

There is a sense of urgency in the responses from IT professionals in public institutions. For instance, 64% of respondents think that increasing the sophistication and breadth of online services in Romania is urgent or very urgent, and only 9% say that we should pace ourselves. The results are consistent with our own experience in interviewing IT experts from public and private institutions, who are almost universally exasperated by the slow pace of innovation in government. This is also evident from the proliferation of civic tech organizations (such as Code4Romania, Geeks4Democracy and others) that try to help public institutions design, implement, troubleshoot and improve ICT solutions to different problems inside communities with more speed than the glacial pace usually encountered in government.

Each Romanian municipality is required by law to have a strategic plan for its development. Electronic government was not mentioned in any of those we found, which is in sync with the low priority that digital transformation is given from the central level of government. Data are also non-

existent regarding the intended recipients of online services: no city hall knows how many of its citizens use the internet and how (for example, what is the percentage of mobile users, to be able to design services accordingly), what the level of digitalization of companies and especially small and medium enterprises is (which would benefit most from an easing of the bureaucratic burden) and what the served citizens or companies would want. This dearth of data is encountered not only in small cities and towns, but in big cities also, and is replicated in most Romanian public institutions, not only city halls.

Finally, the gender of respondents is fairly balanced, with 42 percent females and 58 percent males.

5. Testing the hypotheses

One of the starting hypothesis was confirmed, while for two others the answer is more nuanced, the responses suggesting the problems are more complicated than we thought. One was refuted altogether.

The following two tables show the main obstacles encountered by the respondents in implementing online services in their institutions, and the main beneficial factors that help in this goal of digitizing local government in their communities (the grades are from 1 to 5, with five being the highest value).

	Average score
Lack of financial resources	4.20
Difficulty in competing on pay with private companies	4.00
Lack of trained personnel	3.95
Lack of interinstitutional interoperability	3.78
Lagging internal IT infrastructure	3.71
Outdated internal procedures	3.66
Obsolete internal structure of the city hall	3.55
Lack of management support	3.50
Lack of openness and transparency	3.22
Lack of public pressure	3.07
Lack of immediate results	2.95
Slow internet connections	2.89

Table 2: The most important obstacles in implementing online services in Romanian public institutions

	Average score
Well-trained people in the IT department	4.37
Management support	4.30
Legal constraints	4.24
Sufficient ITC equipment	4.23
Sufficient financial resources	4.22
Good relationships with ITC and digital solutions providers	4.13
Citizen's increasing usage of private online services	3.74
Ties with other public institutions	3.72
Obtaining visible results fast	3.65
Rethinking internal processes	3.49
Pressure from the public	3.17
Internal reorganization of the city hall	3.13

Table 3: The most important beneficial factors helping online services implementation

First hypothesis: *Romanian public institutions (in our case, City Halls) experience difficulties in having IT positions filled.*

This hypothesis is confirmed by the responses we collected. Managers are having difficulties filling ICT positions in their institutions, and they are aware that this is an important problem – the highest average marks of all the beneficial factors was having well-trained people in the institution's IT department. From discussions with people that filled in the questionnaire, we found out that the reasons that small cities and towns are having trouble finding good people for specialized positions are, if anything, more insoluble that those encountered in big cities.

Public administration organizations in small cities and towns find that they have to fight for an increasingly smaller number of IT professionals (because most of them have moved in bigger cities, where they have better prospects) with private companies that can offer a bigger salary, extra benefits and more opportunities for career development. There is a general lack of trained specialists in all technical fields, but, because of the great expansion in the ICT sector in Romania, these experts are more sought-after than ever. It does not help that small municipalities overwhelmingly lack tertiary education so the best and brightest tend to move for university studies in bigger cities and tend to stay there, snatched by IT companies. Even if there are available job-seekers with the necessary skills, the pay that can be offered by a public institution is stipulated by law and, for people with little or no work experience especially, is pretty low.

A possible answer would be for more governmental institutions to pull resources together and use common solutions developed with interoperability in mind from the start. For this, the legal framework would have to be adapted to accommodate such an initiative and turf wars to be minimized. Civic tech organizations could help too, but they are not a panacea, they are a Band-Aid to be used in select cases.

Second hypothesis: *Management support and internal reorganization of the institution are seen by the IT professionals as very important in e-government development.*

This hypothesis was only partially confirmed. The two items related to this in our question about the obstacles in electronic government development (obsolete internal structure of the city hall, and outdated internal procedures) scored 3.66 and 3.55, respectively, out of a maximum of five. The item in our question about the beneficial factors helping the digitalization of their institution (internal reorganization of the city hall) scored dead last – 2.5 out of five. This has to do also with the lack of authority of the head of the IT department from within the institution (for example, heads of other departments can usually buy hardware and software without the approval of the specialists in the institution). Because there was, in the vast majority of cases, no study about the internal processes and workflows of the organization, there is no theory about how these could be redesigned and improved.

Because of this lack of clout of the IT professionals inside public organizations, it comes as no surprise that management support comes at the top of perceived beneficial factors. In a hierarchical organization such as a Romanian city hall, power and authority come from the boss (the mayor); if she or he understands a little about technological change and the transformations it brings and is willing to support such projects, things stand a much better chance to be implemented; if not, their odds of being brought to fruition are usually slim to none.

Third hypothesis: *The main obstacles in e-government development are lack of interinstitutional interoperability and the differences between pay in private versus public organizations.*

This hypothesis was partially confirmed. The two obstacles we expected to impede most were in the top 4 of those ranked by our respondents, but what is perceived as the biggest problem is the lack of financial resources. This worry is bigger in towns than in big cities for a number of reasons: most municipalities in Romania are dependent on money disbursed discretionarily by the central government even for day-to-day operations, not only for investments. This saps projects that span over years and need clear commitments and resources (among them – money) to come to fruition. This only exacerbates the difficulties public institutions face in recruiting good people that can implement digitalization and can design and put into practice solutions to link their databases and software with other governmental organizations in order to offer better services to citizens and companies.

It is true that in 2017 pay in the public sector increased on average, but the difference in pay between the private IT companies and public ones is far from being bridged. Another problem is the lack of attractiveness of public sector jobs: such a career is seen mostly as dull, repetitive and lacking personal improvement opportunities. No city hall in Romania had the audacity and the resources to create something like Boston's New Urban Mechanics unit; small cities and towns can only dream of something like that.

The fourth hypothesis: *Public pressure is an important factor in implementing electronic government.*

This hypothesis was not confirmed. Both in our list of obstacles in electronic government implementation and in that of beneficial factors that could help digitalization, the item related to public pressure was ranked in top three from the bottom. This surprising (for us) result may have to do with the lack of established communication channels between local public institutions and the communities they serve. Changing this culture, reinforced throughout the communist times, is hard. Governmental organizations are mostly insulated from the public and they find it hard to fathom

that people or companies might have an important role to play in devising and implementing public policies.

The first signs of change started to appear (a number of city halls have started participatory budgeting projects, for example), but these changes are taking place predominantly in big cities. It does not help that the average level of digital skills in small municipalities is lower than in big ones, and people are not that familiar with what can be achieved with the help of new technologies.

6. Limitations and further research

The results could be refined by conducting in-depth interviews with some of the respondents, because the responses could, in this way, be greatly expanded, and the insights gathered greatly enriched. Another avenue of research is collecting responses (through surveys, interviews or both) from other types of local public institutions besides city halls and seeing if things differ in one way or another in other parts of the government.

At the same time, responses collected from IT professionals in central government organizations could bring a different perspective, and possibly shed some light on trends noticed during data collection (for example, the lack of centralized digitalization projects in Romania).

7. Conclusion

It is tempting to berate public servants working in the IT departments in Romanian small municipalities for the slow pace of technology-driven transformation in their institutions. Our opinion is, on the contrary, that they are doing, by-and-large, all that could be expected from them, with the resources they have available. In fact, even the name ”IT department” is a misnomer: in the vast majority of cases, it consists of a single person, and their job is much more one of tech support than designer of the digitalization strategy. The low priority given to electronic government and the respondents’ frustration with this is apparent in most surveys and much more so in the one-to-one conversations we had.

The lack of basic tools to be used in all Romanian governmental organizations that can help with integrating existent or future digital solutions (for example standards or national registries, to name but two) is a big hurdle and it will plague electronic government in Romania for as long as it will stay valid.

8. References

[1] AL-BUSAIDY, M., & WEERAKKODY, V. (2010) E-Government Implementation in Oman: A Comparative Study of Three Public Agencies. AMCIS.

[2] ANTHES, G. (2015) Estonia: a model for e-government. Communications of the ACM 58(6), 18-20.

[3] BIASIOTTI, M. A., & NANNUCCI, R. (2004) Teaching e-Government in Italy. Electronic Government: Third International Conference. Zaragoza.

[4] COURSEY, D., & NORRIS, D. F. (2008) Models of e-government: Are they correct? An empirical assesement. Public Administration Review 68(3), 523-536.

[5] DUKIC, D., DUKIC, G., and BERTOVIC, N. (2017) Public administration employees' readiness and acceptance of e-government: Findings from a Croatian survey. Information Development 33(5), 525-539.

[6] EVANS, D. & YEN, D.C. (2006) E-Government: Evolving relationship of citizens and government, domestic, and international development. Government Information Quarterly 23(2), 207-235.

[7] HOLDEN, S. H., NORRIS, D.F & FLETCHER, P.D. (2003) Electronic Government at the Local Level. Public Performance & Management Review, 325-344.

[8] KATSONIS, M. (2015) Digital Government: A Primer and Professional Perspectives. Australian Journal of Public Administration 74(1), 42-52.

[9] KUMAR, V., BHASKER, M., BUTT, I. & PERSAUD, A. (2007) Factors for Successful e-Government Adoption: a Conceptual Framework. The Electronic Journal of E-Government, 63-76.

[10] LIU, Y., CHEN, X. & WANG, X. (2010) Evaluating Government Portal Websites in China. PACIS 2010 Proceedings.

[11] NORRIS, D. F. & REDDICK, C.G. (2012) Local E-Government in the United States: Transformation. Public Administration Review 73(1), 165-175.

[12] REDDICK, G. (2004) Empirical models of e-government growth in local governments. E-Service Journal 3(2), 59-84.

[13] ŞANDOR, S. D. (2012) ICT and Public Administration. Transylvanian Review of Administrative Sciences, 155-164.

[14] United Nations. United Nations E-government Survey. 2016. (2018, January 5). Retreived from http://workspace.unpan.org/sites/Internet/Documents/UNPAN97453.pdf.

[15] URS, N. (2016) Online Services and Social Media Use in Romanian Cities: Can We See a Pattern? 24th NISPAcee Annual Conference, Spreading Standards, Building Capacities: European Administrative Space in Progress. Zagreb.

[16] WANG, F. (2014) Explaining the low utilization of government websites: using a grounded theory approach. Government Information Quarterly 31(4), 610-621.

STATE OF DIGITAL LITERACY: PREPAREDNESS OF HIGHER EDUCATION STUDENTS FOR E-ADMINISTRATION IN HUNGARY

László Berényi[1] and Péter László Sasvári[2]

DOI: 10.24989/ocg.v331.29

Abstract
Taking the advantages of electronic administration requires a comprehensive development program. Beyond the technical background, databases and user interfaces, it is necessary to consider personal aspects including preparedness of users and administrators. Increasing the confidence in e-administration is difficult to reach without their advanced IT and ICT competencies. The main challenge can be formulated as improving digital literacy. If receptiveness for novel technological solutions fails, efforts may become redundant. Successful actions in this field are not available without the thorough analysis of present state and critical knowledge elements. The paper summarizes some results of a diagnostic analysis about the ICT utilization in order to establish further research actions about task-technology fit in the field. Research sample consists of public administration students who will play an important role in realizing e-governance. Results show that technical background, as well as general utilization of ICT tools, are no more bottlenecks of success; however, there are relevant education challenges on developing digital literacy.

1. Introduction

Developing e-solutions is a key driving factor both for business and public administration. There are fundamental changes both in official administration and personal communication. The virtualization of our life became general; information technology (IT) and info-communication tools (ICT) integrate everyday activities [13]. ICT tools represent the link between the knowledge and skills and the user, however, the ability to use them is also inevitable. Consequently, establishing successful solutions instead of generating more problems requires a comprehensive set of actions including an info-communications strategy, supporting the development of hardware elements and networks as well as solving education challenges. The last one covers improving the users' skills and increasing the level of acceptance. There is a need for a technological development (see [16]) that assumes the evolution of digital literacy in parallel with technical development. Digital literacy enables us to match the medium to the information presented and to the audience targeted [12]. Eshet-Alkalai [6] defined the term as "survival skill in the digital era" referring to the context and responsibility of formal education. Furthermore, the present students will enter the labor market within a few years that will generate additional tasks that are expected to be solved through digital literacy and open new aspects of the digital world to learn.

2. Task-technology fit

Quality evaluation models summarized by Isaias and Issa [11] may support to monitor the progress of IT and ICT-related development and to designate intervention points in order to achieve strategic

[1] National University of Public Administration, Institute of E-Government, berenyi.laszlo@uni-nke.hu
[2] National University of Public Administration, Institute of E-Government, sasvari.peter@uni-nke.hu

goals. There are various frameworks and models developed in the past decades with some common characteristics:

- environmental factors are considered,
- attitudes and/or intention to activities are involved,
- there is a feedback mechanism that may confirm the usefulness of the activities.
- assumes that the solution is available and knows by the user.

There is another approach is presented in the task-technology fit models (see [11], [5]) with the core idea that performance and satisfaction can be evaluated in the knowledge of task characteristics (similarly to the product-based approach of quality [7]). Task-technology fit can be understood as a quality indicator of a technology meeting the current requirements. There are several approaches; even the original interpretation [10] includes more models (Figure 1), but the scope of revisions is rich (see e.g. [4], [8], [11]).

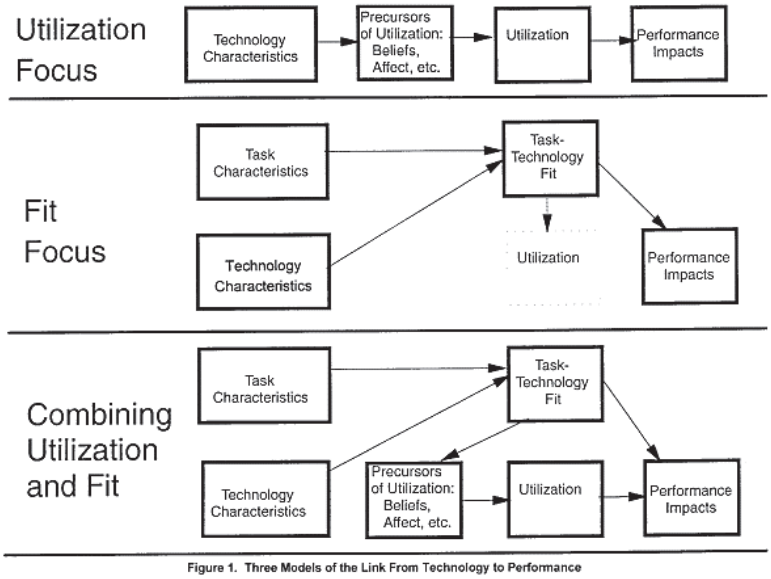

Figure 1: Three models of the link from technology to performance [10]

3. Research goals and sample

Goodhue and Thompson [10] draw attention to the limitation that task-technology fitting (fit focus model) is difficult measure in general since utilization is a complex outcome; however, it may be worth to perform an analysis with a wider focus to prepare further research. Our paper attempts to review some aspects of the task-technology fit of ICT tools use among public administration higher education students. Obviously, each task requires an individual analysis, however, we believe that the task-technology fit models, especially the approach of the fit focus model are suitable for

evaluating the progression. This needs the general categorization of the tasks and the review of the available technological background. Currently, a detailed analysis based on the task-technology fit model is not feasible, the purpose of the paper is to designate the basis of a further research model in the field.

The paper deals with following issues:

- technology characteristics is described based on the statistics on the availability and the utilization of ICT tools and networks by the recent reports of the Hungarian Central Statistical Office in the field;

- task characteristics aims to collect frequent tasks performed by ICT tools;

- performance is concluded based on personal satisfaction and some competencies.

This pilot investigation aims the public administration higher education students of the National University of Public Service since their competencies as both users and providers are a key success factor of the efforts on developing e-administration. A deeper analysis of the field is necessary since digital literacy of them may be considered as a key driving force of enhancing the e-government. Computer use is evident in the target group, these students can be considered as frequent ICT users. The method of the investigation used a self-filling survey managed by the EvaSys e-survey system. Statistical analysis allows checking whether the virtualization and utilization of the mobile/portable ICT tools play an increasing role in their life that may contribute to the acceleration of the related development efforts.

The target group included the students of the subject 'Public administration information technology and information systems II". There were 243 full-time and 111 part-time students learning this subject in the fall of 2017. Each student received a message through the study administration system, including a link to the questionnaire. The participation was voluntary. 12.7% of the students answered the questions. The research sample consists of the answers of 45 bachelor level students. 77.8% of them are females; 71,1% are full-time students. The representativeness of the sample is not assured, interpretation of the figures and findings are limited to the sample. However, these results allow establishing questions related to the availability of the technology and the utilization of the technology.

4. General ICT availability and utilization

4.1. General trends in household use

Reports of the Hungarian Central Statistical Office (KSH) in the field prove a clear improvement in computer usage among households [20]. 76% of the population were effective (active) computer users in 2015, i.e. they used a computer at least once in a three-month period. While the indicator is lower than the EU average (83%), a continuous increase can be observed in comparison with the previous years. 56.8% of the households had a desktop computer in 2009 and this ratio had barely changed to 2013 (58.3%). Nevertheless, the share of portable computers has been growing steadily; the ratio has changed from 21% to 41.6% in the period.

Using ICT tools is usually associated with using the Internet. The growing number of households with Internet access is a positive tendency (2009: 55%; 2012: 69%; 2015: 76%).

The KSH report on telecommunications, Internet and TV services [1] pointed out that there were 9.1 million Internet subscriptions in Hungary in the 2nd quarter of 2017. It is to note, that is a five times increase over 10 years. Wired internet bandwidth has begun to grow dynamically; 75% were over 2 Mbit/s, 49% over 10 Mbit/s and 14% over 100 Mbit/s in 2016. The ratio of the latter category exactly doubled from the same period of the previous year. Development of data traffic on the wired Internet is remarkable. The traffic was about 383 thousand Terabytes, which means a 34% increase over one year. Expansion has accelerated, which is proved by the fact that the value of the indicator was 39 thousand Terabytes in 2014 fourth quarter and 14.4 thousand Terabytes in 2010 fourth quarter based on data from KSH [19].

Furthermore, Internet subscriptions included 6.3 million Mobile Internet subscriptions. The most popular activities on the Internet are summarized in Table 1.

	2014	2015	2016
Sending and receiving emails	93.4	93.0	91.7
Internet telephony	52.7	54.7	53.6
Visiting social sites	79.3	83.4	82.8
Reading news	85.6	85.7	88.1
Information search for goods and services	13.6	83.3	88.0
Sharing own content	14.4	58.1	45.6
Internet banking	40.3	46.4	44.5

Table 1: Internet utilization among active computer users (%) [1]

4.2. General trends in corporate use

Sasvári [17] analyses the use of ICT tools on the corporate level. According to his results based on an international survey, the level of utilization is diverse, especially with regard to company size. Small- and medium-sized companies were lagging in using information systems [18]. Of course, this does not entail the total neglect of IT services and ICT tools, but the depth and scope of utilization are fairly questionable.

More than four-fifths of the corporations in the sample have a web page in 2010 and they used the Internet for advertising products and services. 60% of micro- and small companies have had a product or service advertised on the Internet. Moreover, internet banking was taken advantage of by 80% of micro and 85% of small companies.

Official statistics confirm Sasvári's findings. 91% of the companies used the Internet in 2013, and 27% of them had broadband Mobile Internet access. However, there are areas for improvement, including:

- low utilization of cloud computing: only 26.2% of large companies (over 250 employees) took advantage of any cloud-based services (the national average ratio is 11.6%),

- corporate web pages focused on product and service information; online ordering was available at 80% of them, however, every third company managed its purchasing also this way,

- an enterprise resource planning system was installed by 70.5% of large companies but by only 37% of medium-sized (50-249 employees) and 12.1% of small firms (less than 50 employees) (KSH 2016).

In my opinion, the reason for this is not mainly the availability of the tools or even the financial possibilities. A large company can define a number of repeatable processes, which are manageable by IT systems, while a smaller company more rarely encounters with equally repetitive challenges. In these cases, individual treatment of the problem with marginal support of ICT can be more appropriate in several ways, including the costs. However, this means that personal IT competencies have fundamental importance in solving the problems.

5. Survey Results

5.1. Time spent with ICT tools

Smartphones and portable computers are the most popular ICT tools what the respondents have (Figure 2). The average time spent with them is about 4.5 hours a day for each. 62.2% of them has a television but only 2.5 hours are spent on it. Desktop computers are held by 42.2% of the respondents, however, daily use is 4.4 hours. The attractiveness of tablets is quite low, but it must be considered that the size of present smartphones is close to tablet-size [2].

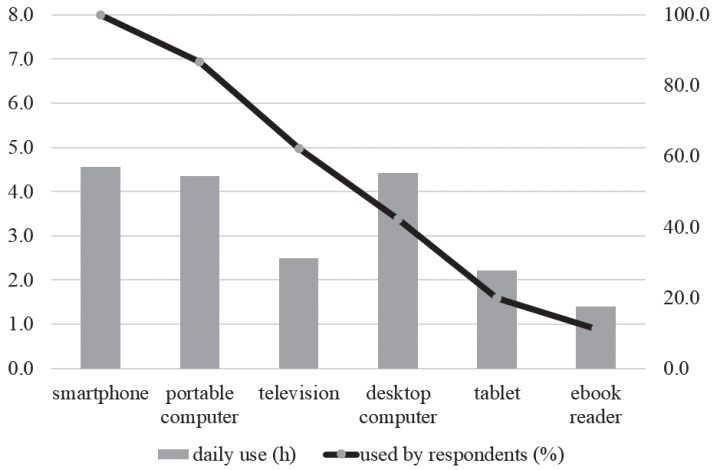

Figure 2: Utilization of some ICT tools in the sample

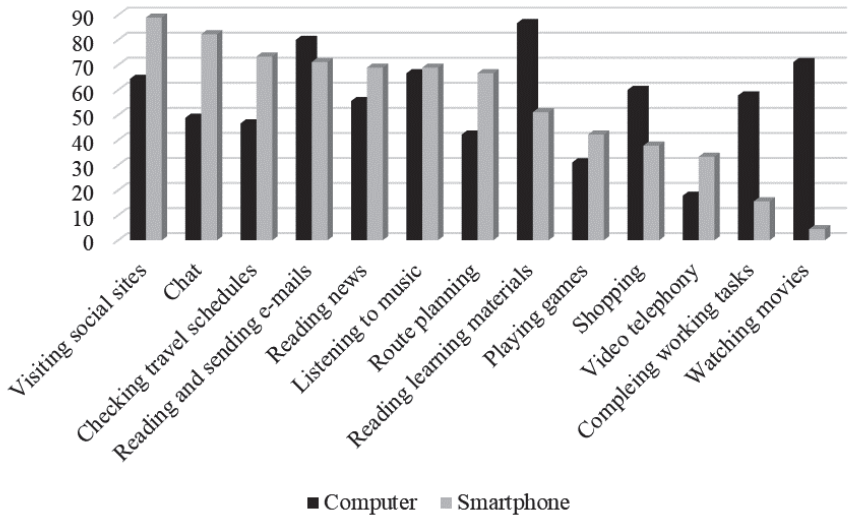

Figure 3: Activities realized with computers and smartphones in the sample (%)

Beyond social presence or e-mails, it is forward-looking that 73.3% uses internet banking, 46,7% uses the client portal of 'Ügyfélkapu'. 91.2% of them buy things on the internet, of which 35.6% oftentimes. The hypothesis of the research says that mobile devices take over the leading role. The survey asked some activities whether it is realized with desktop/portable computers or smartphones. Figure 3 shows that smartphones have a leading role e.g. in case of visiting social sites, chat, reading news and traveling issues. Computers are more popular in case of learning-support, work, shopping or watching movies.

5.2. Competencies and satisfaction

The survey asked the knowledge level about some basic software that may be necessary for the education and working. Based on the respondents' own declaration a very favorable emerges, however it must be added that former experiences [3] show that these answers are biased upward.

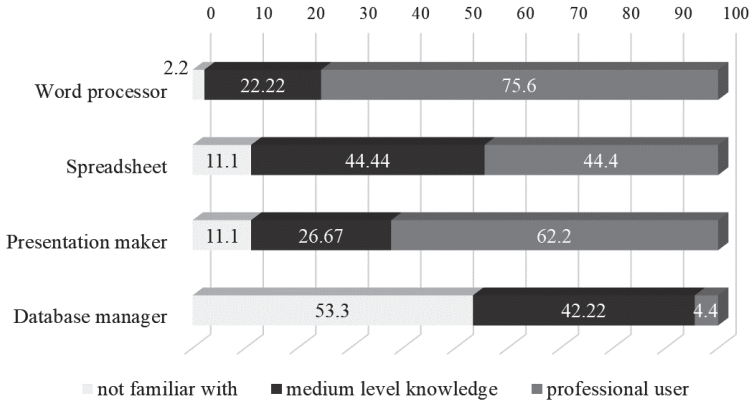

Figure 4: Competencies about office software in the sample(%)

65.9% of the respondents are greatly satisfied with the performance of their desktop/portable computer, and 61.4% with the internet speed. The ratios of dissatisfied ones are 6.8% and 2.3%. A special indicator of the satisfaction is whether people feel computer work exhausting (Figure 5). An additional information is that only 15.6% marked that he or she has a health problem (mainly vision problems) in context with computer work.

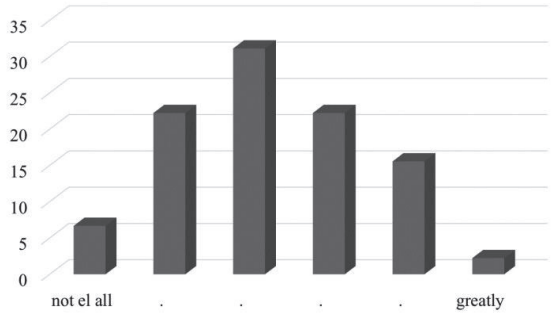

Figure 5: Distribution of the answers about feeling the computer work exhausting in the sample (%)

IT education is inevitable in order to achieve a higher level of digital literacy. The survey asked the respondents to mark their satisfaction with the IT education of various study levels. Results in Figure 6 suggest the need for developing basic education; on the other hand, the performance higher education in this field is encouraging.

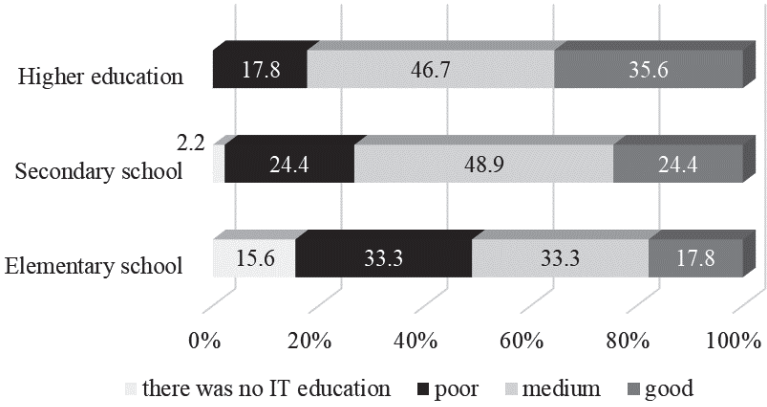

Figure 6: Satisfaction with IT education in the sample (%)

6. Conclusions

6.1. Experiences of the survey

Both national level statistics and the survey results confirm that virtualization and mobilization determine our present. The pilot survey of public administration students show that IT-culture is not alienated from them, their activities are supported by ICT tools on a high level. Present students collect information and keep contact with others primarily through their smartphones.

Considering that governmental development strategy force IT-based solutions (see [14], [15]), it is a progressive building stone that students' knowledge and approach are appropriate. However, the own competencies may be overestimated, and students feel lack of education, their commitment to ICT tools is encouraging. We believe that higher education has the responsibility to integrate work-related skills and competencies with general knowledge.

6.2. Further challenges of modeling

Results show that the availability of ICT tools and IT infrastructure cannot be considered as the bottleneck of e-government services, i.e. the implemented strategic efforts were successful. The future challenge is to designate the effective ways of the utilization.

A practical limitation of the task-technology fit models is that technical elements cannot be evaluated without the accurate definition of the task to fit. Another condition of a comprehensive measurement model is a unified scale-system that was not feasible since that would have been with relevant information loss about the details of opinions.

The research presented in this paper allows defining general performance and utilization factors, moreover the considerable technological background. The survey allows comparing whether computers or smartphones are utilized more often to perform various tasks (Figure 3). Most of the tasks are entertainment-oriented utilization possibilities, work-related ones need further investigation. A separated approach is also suggested by an experience of the survey that is not partially presented in the paper: 81.8% of the respondents are very satisfied with the computer working environment at home, but only 50% of them at the work (18 respondents work full-time, part-time or an internship).

There are two main directions of future modeling:

- However, it would be looking forward to focusing on public administration tasks, this goes beyond the scope of the target group. Task-technology fit model in this scope will require the involvement of IT experts and clients; evaluation of technology, utilization and performance need their opinions.

- Furthermore, tasks that can be investigated directly in the target group are quite common, the work-related tasks are grouped around learning. Using this, we plan to develop a survey for higher education students and to compare the level if digital literacy among different levels and faculties.

6.3. Acknowledgement

This paper has been written with the support of the National University of Public Service in the framework of the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled "Public Service Development for Establishing Good Governance" - Ludovika Digital Governance Research Group.

7. References

[1] Az infokommunikációs technológiák és szolgáltatások helyzete Magyarországon, 2016, Központi Statisztikai Hivatal, Budapest 2017.

[2] BERÉNYI, L., IKT-eszközök használata a jövő munkavállalóinál a Miskolci Egyetem gazdálkodási szakos hallgatóinak példáján keresztül, Közgazdász Fórum, 19, 126 (2016), 3–26.

[3] BERÉNYI, L., Számítógép-használat otthon és munkahelyen – digitális kompetencia és a számítógépes munkakörnyezet ergonómiájának empirikus vizsgálata. Vezetéstudomány. 44, 4 (2013), 51-62.

[4] D'AMBRA, J., WILSON, C. AND AKTER, S., Application of the task-technology fit model to structure and evaluate the adoption of Ebooks by academics. Journal of the American Society for Information Science and Technology, 64, 1 (2013), 48–64.

[5] DISHAW, M. T., AND STRONG, D. M., Extending the technology acceptance model with task–technology fit constructs, Information & Management, 36 (1999), 9–21.

[6] ESHET-ALKALAI, Y., Digital literacy: a conceptual framework for survival skills in the digital era, Journal of Educational Multimedia and Hypermedia. 139, 1 (2004), 93–106.

[7] GARVIN, D. A., Managing Quality: The Strategic and Competitive Edge, The Free Press, New York 1988.

[8] GEBAUER, J., SHAW, M. J., AND GRIBBINS, M. L., Task−Technology Fit for Mobile Information Systems. Journal of Information Technology. 25, 2 (2010), 259–272.

[10] GOODHUE, D. L., AND THOMPSON, R. L., Task-Technology Fit and Individual Performance, MIS Quarterly, 19, 2 (1995), 213–236.

[11] ISAIAS, P., AND ISSA, T., High Level Models and Methodologies for Information Systems, New York, Springer 2015.

[12] LANKSHEAR, C., AND KNOBEL, M., Digital Literacies – Concepts, Policies and Practices, Peter Lang, New York 2008.

[13] LÜKŐ I., Az információs és a tanuló társadalom, Iskolakultúra, 13, 3 (2003), 102–110.

[14] NEMESLAKI, A., The Theory of "IT-Government" Alignment: Assessement of Strategic Fit in Hungary's Case. Proceedings of the Central and Eastern Europen eDem and eGov Days 2016, May 12-13, 2016, Budapest, 85–92.

[15] ORBÁN, A., A közigazgatási informatika alapjai, Nemzeti Közszolgálati Egyetem, Budapest 2013.

[16] PATAKI, B., Technomenenedzsment, L'Hartmann, Budapest 2014.

[17] SASVÁRI, P. L. Az információs rendszerek kisvállalati alkalmazásának vizsgálata, magyar- és horvátországi összehasonlító elemzés. Vezetéstudomány, 43, S.I. (2012), 56–65.

[18] SASVÁRI, P. L., AND WOLF, R., Austria and Hungary: Different stages of readiness to create added value by using business information systems, Pro Publico Bono - Magyar közigazgatás, 2, 3 (2014) 169–178.

[19] Távközlés, internet, 2014. IV. negyedév, Budapest, Központi Statisztikai Hivatal 2015.

[20] Távközlés, internet, televíziószolgáltatás, 2016. III. negyedév, Központi Statisztikai Hivatal, Budapest 2016.

eDemocracy and Open Government

DEMOCRACY AT THE ONE-CLICK DISTANCE: IS ELECTRONIC VOTING THE BEST OPTION FOR MOLDOVA?

Ina Vîrtosu[1] and Ion Guceac[2]

DOI: 10.24989/ocg.v331.30

Abstract

Electronic voting, known as e-voting, has become increasingly popular in our fast developing technology-driven world. Hence, the Republic of Moldova is a source country of migrants, a significant number of citizens reside abroad. Therefore in most of cases Moldovan citizens have to cast their vote in other countries when Moldova has to hold its elections. Presidential elections from 2016 showed that a poorly organized electing process could lead to violations of constitutional political rights. Hundreds of citizens that travelled a long journey to London, Bologna, Milano and other cities, where polling stations were located, were not able to cast their vote because election officials did not send enough ballot papers. For a country with a numerous Diaspora, e-voting could be a solution for all problems that Moldovans have related to the exercising of voting right. The process is seductively simple, but it is also shockingly vulnerable to different problems - from software failure to malicious hacking - and also requires some special conditions for its implementation. This paper aims to provide an insight into the issues of e-voting, and the debate of pros and cons surrounding it, in order to assess if this solution is the best way to go for Moldova.

1. Introduction

Nowadays many democracies are using or considering introducing electronic voting (e-voting) system with the intention to improve their electoral process. E-voting is often seen as a modern tool for advancing democracy that can increase the overall efficiency of the electoral process. Properly implemented, e-voting can eliminate certain inconveniencies for citizens, such as long distance from polling stations by improving accessibility, speeding up the processing of results, and even reducing the cost of elections/referendums in the long-term.

In May 2008 the Parliament of the Republic of Moldova approved the Law no. 101 on the State Automated Informational System „Elections" (SAISE) [24]. The long-term objective of the SAISE is to achieve full automatisation of the elections in the country. This includes the possibility to vote in any polling station, to vote through electronic voting machines, and/or possibility to vote via Internet. According to the Law No. 101, the e-voting system has to be developed, tested and piloted by the Moldovan authorities by 2018 Parliamentary Elections.

For the Republic of Moldova - a country with a numerous Diaspora - e-voting could be a solution for all problems related to the exercising of voting rights, however from other countries' past

[1] Institute of Legal and Political Research of Academy of Sciences of Moldova, 1 Stefan cel Mare Bld., Chisinau, Republic of Moldova, ivirtosu3@gmail.com, http://icjp.asm.md/; University of Macau, Avenida da Universidade, Macau, yb67199@umac.mo, http://www.umac.mo/

[2] Academy of Sciences of Moldova, 1 Stefan cel Mare Bld., Chisinau, Republic of Moldova, ion.guceac@asm.md, http://asm.md/

experiences not all e-voting projects succeed in delivering on such high promises. An easy voting process that allows citizens to cast ballots the same way they buy items from Amazon, or punch in a PIN code to check out at the grocery store is not as simple as it looks. You could click on a candidate from a home computer or use a touch screen device at the local polling place; however, we have to understand that the current e-voting technologies are not problem-free. Particularly, in Moldova the decision of going paperless could face not just numerous legislative and technical challenges, but also other problems that raise a lot of scepticism, related to the process, or even social or political opposition to the introduction of new voting technologies.

Concerns related to e-voting are linked to the complexities of these electronic systems and procedures related to them [1]. Many e-voting solutions lack transparency for voters, and they are only completely understood by a small number of experts. In these circumstances, the integrity of the electoral process relies largely on a small group of system operators instead of thousands of poll workers. The process has to be carefully planned and designed; otherwise the introduction of e-voting can undermine confidence in the whole electoral process. Hence, it is of crucial importance to analyse all premises and circumstances, to devote adequate time and resources for considering correct e-voting implementation, and take into account other countries previous experiences.

E-voting is probably one of the most controversial methods of expression at the ballot boxes. If Estonia and Brazil consider it a system that works well and is acceptable for its citizens to express their constitutional rights, some countries, such as the Netherlands, Finland, France, and Germany believe that the use of online technology for voting is not safe and raises numerous constitutional problems, or uncertainty in the expression and quantification of votes. Norway even has dropped tests because of security hazards.[3]

All technology upgrades projects in the elections process require careful deliberation and planning [17]. Voting is a process at the heart of a democratic society, and represents the most responsible stage of the electoral process. It is the „outcome" of the entire electoral campaign, therefore introducing e-voting is probably the most difficult upgrade as this technology touches the core of the entire democratic process in the country - the casting and counting of the votes. This electoral option provides an opportunity for solving some old electoral problems, but also introduces a whole range of new concerns [17]. As a result, e-voting implementation always triggers criticism and opposition, being one of the most disputed information technology application in elections.

Our paper does not have intention to provide guidelines for the successful introduction of e-voting in the Republic of Moldova however presents some of the premises, concerns, and challenges related to this technology that have to be taken into account in the implementation process.

[3] The Institute of Social Research in Norway conducted a study in which voters express their concerns related to the secrecy of their vote, which they see as a compromise of their democratic rights. In addition, voters' fears are embedded in the encryption system that guards the privacy of their votes, in special voters are not sure if their votes are safe from hackers.

2. Defining Internet Voting

E-voting systems have been in use since the 1960s,[4] with the first punched card systems. From then e-voting technology evolved and includes: a) voting using ballot papers, with special ballot boxes and scanning machines installed, so the ballot can be scanned before falling into the ballot box, or voting counting using handheld scanning devices (as „e-Pen" technology), used to digitally identify marks on the ballot papers; b) voting using dedicated electronic devices (voting kiosks); c) voting with transmission of ballots and votes via telephones, private computer networks, or Internet.

A Feasibility Study for the Internet Voting (Study) [34], conducted in Moldova for Central Electoral Commission (CEC) to evaluate the possibilities of introducing modern voting technologies in elections, culminate with the conclusion that the best e-voting solution for the country is the remote *Internet Voting Information System* (IVIS or i-Voting) that should be owned and managed by the CEC as a Module of the SAISE based on the *Reliable voters list* (SRV).

The current voting system is not adequate for Moldovan citizens living abroad, and there is a sufficient demand for the remote i-Voting which would facilitate voting process for Diaspora, since voters residing abroad won't benefit from other methods of e-voting, such as e-voting machines or ballot scanners.

In new democracies, Diaspora has a powerful and sound voice in the development of the country of origin. When it comes about Diaspora, different numbers are presented however according to the NEXUS data [7] currently there are approximately 700,000 Moldovan citizens residing or living abroad. Among them, more than 450,000 are long-term migrants (majority - labour migrants); over 100,000 are permanent migrants, and over 150,000 of Moldovans abroad are seasonal migrants. Majority of potential voters are residing in Italy, Russia, France, UK, Canada, USA, Spain, Portugal, Greece, Germany, Belgium, Turkey, and Israel [4].

To understand why this option was selected as the most optimal for Moldova we need to define and understand the concept of i-Voting.

Internet voting (i-Voting) refers to a voting method that transmits voted ballots via the Internet through a web browser or client application, accessed through an Internet connected personal computer, smartphone, or tablet [8]. Two main types of i-voting can be identified:

1. *On-site i-Voting,* which is physically supervised by representatives of governmental or independent electoral authorities, conducted at controlled settings (voting places or kiosks, established in high-traffic areas);

2. *Remote i-Voting*, without going to a polling station, and allows voters to transmit their voted ballot from any Internet connected device they have access (e.g. public/home/office computer, tablet, smartphone).

i-Voting greatly reduces direct human control and influence in this process, however on-site i-Voting allows electoral administrators to exercise greater control over the voting infrastructure used

[4] Their first widespread use was in the USA where 7 counties switched to this method for the 1964 presidential election. The newer optical scan voting systems allow a computer to count a voter's mark on a ballot.

in the elections. At the same time remote option is particularly attractive as it does not require voters to go somewhere to vote, and thus potentially reduces costs and maximises the convenience for voters [8].

3. Is Moldova ready for Internet Voting?

According to the Study, remote voting via Internet is the best option as it may increase public trust in the public sector and government e-services, increase accessibility to vote for people with disabilities and limited mobility, reduce cost per voter, and most important to solve the problem of participation of Moldovan citizens living abroad [33]. The Study emphasizes that Moldova needs the following prerequisites for i-Voting implementation: necessary legal framework, social approval and demand, adequate technological maturity and political consensus.

3.1. Necessary legal framework

The legal framework needs to be reviewed to ensure fundamental rights and duties for democratic elections to be in line with international and regional commitments subscribed by the Republic of Moldova. These references might be interpreted differently in an e-voting context and require harmonization with the technology choice that the country wants to implement [17].

In the Republic of Moldova the creation of e-voting was assigned in the regulatory and legislative acts. However, there is no specific regulation of e-voting in the Constitution of the Republic of Moldova: Article 38 just mentions that the basic election principles must be ensured [5].

The Electoral Code had some modifications according to which starting from 2015 the State Register of Voters was implemented – a unique integrated information system of voters evidence, accomplished on the basis of the State Register of Population, drafted and approved by the law on the concept of SAISE, but does not include yet specific provisions regulating i-Voting concept, policies, voting secrecy assurance principles, voting procedure, rules, such as vote verification and cancellation, voter identification, and other characteristic components for this system. Also, there are no provisions on remote voting from an uncontrolled environment. In this context, the Electoral Code has to be modified by introducing i-Voting concept, procedure, including security and audit requirements, and other essential elements for this voting procedure.

Legal implications should go beyond the electoral law and fundamental obligations for democratic elections; it also has to cover parallel or subsequent legislation, such as digital identity, digital identification, digital signatures, data protection etc. In order to create a proper legal framework for the implementation of i-Voting, Moldova has already implemented some of necessary laws: Law on registers [22], Law on informatisation and State information resources [21], Law on electronic signature and electronic document [25], Law on personal data protection [24], Governmental Decision on the implementation of electronic identification document [12], Government Decision on the integrated electronic service for authentication and access control (MPass)[5] [13],

[5] MPass or integrated electronic service for authentication and access control is defined as a reusable service, hosted on the Joint Governmental Technology Platform (MCloud), which aims to provide an integrated, secure and flexible mechanism for authenticating and controlling users' access to information systems, including electronic services.

Governmental Decision on the governmental integrated electronic service for electronic signature (MSign)[6][14] etc.

3.2. Social approval and demand

In 2012 Moldovan emigrants from 11 countries submitted a petition to the state authorities asking for the implementation of the e-voting procedure or correspondence voting, which, according to them, will make a major contribution to the growth of the number of voters outside the country and will allow Moldovan emigrants to exercise their constitutional right to vote [26]. The document was signed by 29 Diaspora associations, however the views of Moldovans appear to be divided in terms of modern methods of exercising the right to vote; some of them signed a petition on correspondence voting and did not agree with e-voting, others signed for e-voting as well. Those who did not sign for e-voting explained that many expatriates do not understand the process and are afraid of frauds.

Public trust is a very important element built on the socio-political context in which e-voting is introduced [17]. A negative social opinion creates serious risks, even if the e-voting technical and operational foundations are reliable and sound. Although, the government may ensure transparency and make available to voters all necessary documents, it will not be possible for everybody to understand an e-voting system. To have confidence in the electoral process, many voters rely on others who are in a position to understand the materials and processes. Social actors, such as non-governmental organizations (NGOs), information and communications technology (ICT) security expert groups (as well as other experts), and media, often have strong influence on public opinion, therefore these actors should be included at the early stage of the implementation of e-voting, by providing them with ample information about the system, that can be disseminated, and allowing them to clarify their own and citizens' concerns. It is important to hear and address their concerns by clarifying all misunderstandings, correcting weaknesses or accepting certain risks as a trade-off for the benefits of implementation of the new system. A supportive society could significantly help the introduction of e-voting and can temporarily even cover up problems that may occur in the detailed technical implementation.

In 2016 was conducted an on-line Survey[7] among the Moldovan Diaspora representatives on the introduction of i-Voting in the Republic of Moldova. The Survey revealed that at the 2016 Presidential elections 37% of the respondents did not participate just because the polling station was too far, 92.8% declared their support to the introduction of i-Voting, and 96.1% of supporters indicated that they would like to vote over Internet during the next elections. The Survey has proved that the current voting system is not adequate for Moldovan citizens living abroad, and there is a sufficient demand for the remote voting solution which would facilitate voting for the expatriates.

---

[6] MSign or integrated electronic service for electronic signature is a reusable service, provided at the level of the Joint Governmental Technology Platform of the Government, which aims to provide a secure, flexible and flexible integrator mechanism for various solutions for the application and verification of the authenticity of the electronic signature by users provided by electronic signature providers in accordance with the legislation.

[7] The Survey was prepared and disseminated on April 2016 on Google Forms by the UNDP consultants mainly via the social networks with assistance from the Bureau for Relations with the Diaspora, Moldovan Government and UNDP Programme. The survey was addressed to Moldovan citizens living abroad and 914 citizens participated. Generally, the majority of the Internet users and consequently of the i-Voting supporters are aged between 25 and 45 years old (i.e. 71,2%) and between 18 and 25 years old (i.e. 19,4%). About 11% of the respondents indicated that they are older than 45 years.

3.3. Adequate technological maturity and necessary „infrastructure"

Choosing the right voting technology is essential as the technology needs to operate reliably within the available infrastructure, taking into account the prevailing environmental conditions. For the implementation of i-Voting, the Internet penetration, mobile network coverage, technical infrastructure, level of ICT literacy in the country, necessary quantity and quality of technology experts/managers with sufficient experience and competences are more than necessary. Even having all these prerequisites the ICT component should be implemented with a high level of transparency that generates broad stakeholder confidence.

According to the official data presented by the International Telecommunication Union (ITU) in 2016, 76% of the households in Moldova have access to the Internet, 75% - access the Internet at least once a day [18]. The penetration rate for the Internet service in 2017 is around 71% (over 2.87 million users) [19]. At the same time the mobile telephone penetration rate is 123% (over 4.44 million users. According to the statistical data presented by ANRCETI[8] on the three providers of mobile communications networks and services (Orange Moldova, Moldcell and Moldtelecom - Unite), the number of users who accessed the Internet based on 3G technology amounted to 1.622 million, with a penetration rate of broadband mobile Internet access services of 60% [2]. At the beginning of 2017, the 4G coverage rates of the territory and population of the Republic of Moldova were 94% and 97%, respectively [16]. The figures clearly show that Moldova has a high penetration rate of Internet and very good mobile coverage. Internet is also accessible almost everywhere in the country. Mobile phones, tablets and computers can be found in the majority of households.

In 2014 in Moldova was launched the electronic identity card of the citizen (E-ID card)[9] [12] that allows the practical accomplishment of the e-voting system. The identity card with incorporated electronic chip and digital signature as a unique electronic identification and authentication device will allow the e-voting via Internet (but also can be used at the voting machines which will be installed at the polling sections), regardless of the voter's location. The document is also integrated with the e-Government solutions, MPass and MSign platforms, and allows drawing up legal documents in electronic format, to access information from the informational systems and resources, the processing of the public and private electronic services, and financial transactions accomplishment.

As a newly launched product it is obvious that not many citizens have E-ID. Moreover the cost of this document is five times higher than the cost of a simple identity document.[10] Therefore for the purposes of i-Voting in Moldova, it is advised to use several different methods of voter authentication, such as MPass service using mobile signature/ E-ID cards/digital certificates, or a special login credential (a pair of login passwords), generated and delivered for the voter on a dedicated subpage within a CEC website

[8] National Regulatory Agency for Electronic Communications and Information Technology of the Republic of Moldova
[9] The model of the electronic identity card of the citizen (E-ID card) can be seen on official page of public institution „Public Services Agency", http://www.registru.md/en/node/3337. The service can be ordered online on http://e-services.md/?q=ro/content/buletin-de-identitate-electronic.
[10] The price of the electronic identity card produced during 30 days is 700 lei (around 34 euro), and the price of the identity card – 130 lei (around 6.4 euro).

3.4. Political consensus

The introduction of new voting mechanisms requires changes in the legislation, therefore consensus and sustained multiparty political acceptance is a mandatory ingredient. E-voting systems can be most easily introduced when there is a long-term support of the majority of political parties. In the opinion of some experts, some political actors may oppose e-voting for many different reasons, either because they have real technical concerns, or they fear that the new voting channel is an advantage for their political opponents, or just because they do not have confidence in the independence of those implementing the system [11,17]. Parliamentary political parties expressed a general support for the introduction of i-Voting in Moldova. Members of Parliament mentioned that i-Voting could be an alternative voting solutions for citizens living abroad, young electorate whose participation rate in the elections is very low, and for those who usually are not able to vote due to other agendas during the Sunday Election Day [34].

4. Strengths and Weaknesses associated with Internet Voting

The discussions about e-Voting are very arduous and contradictory; debates among scholars, politicians and experts, revolving mainly around pro and cons of the implementation of this project. As i-Voting more directly affects two large groups - the voters and the government - in order for i-Voting to be instituted, it must be a significant advantage, much greater than the costs for both of these groups.

4.1. Why Internet Voting should be implemented?

We can mention the following strengths associated with e-voting: a) potentially increased participation and turnout, particularly with the use of i-Voting[11]; b) increased convenience and accessibility for voters, being more attuned to the needs of an increasingly mobile society, especially increasing the ease of voting for citizens who are geographically isolated from election centres; c) efficient handling of complicated electoral systems formulae, subsequently faster vote count and tabulation [17]; d) possibility of multilingual user interfaces that can serve a multilingual electorate better than paper ballots, especially in case of the multicultural society of the Republic of Moldova; e) increasing accessibility to vote among people with disabilities and those with limited mobility; f) more accurate results as human errors are excluded; g) long-term cost savings (in poll worker time, reduced costs for the production and distribution of ballot papers, reduction of spoilt ballot papers as voting systems can warn voters about any invalid votes, global reach with very little logistical support, no shipment costs, no delays in sending out material and receiving it back etc.); h) reduced number of incidences of vote-selling and family voting by allowing multiple voting where only the last vote counts, and prevention of fraud in polling stations during the transmission and tabulation of results by reducing human intervention.[12]

[11] Estonia has seen positive movement in turnout since the introduction of Internet voting. Prior to the introduction of Internet voting, 58.24 % of voters participated in the 2003 parliamentary election. After the introduction of Internet voting in 2007, turnout increased to 61.9 %, and again to 63.5 % of voters in elections held in 2011.

[12] The system must generate cryptographic verification proofs (e.g. voting receipts). Indeed the price of one bona fide, for registered Moldovan vote varies from place to place, however the last years' elections show that election frauds require extensive efforts against illegal voters, election-fraud cases more often involve citizens who sell their votes, usually remarkably cheaply at 100 MDL and at the high end, corrupt candidates who use money, goods and influence to get more votes.

i-Voting can reduce this common practice and serious issue for Moldovan elections, such as practice of buying voters, blocking the electoral process through lack of ballots, electoral tourism – all attested even for the last Presidential elections. As a result, elections were followed by protests in the Republic of Moldova, Romania, and other European countries, demanding the recount of votes and even a third round of elections.

4.2. The challenges of i-Voting implementation

Besides strengths and positive sides of i-Voting implementations we should also take in account a range of shortcomings as i-Voting faces a wide variety of potential attackers beyond those encountered in traditional elections and these include: insider attacks from system administrators, cybercriminals working for dishonest candidates, so-called „hacktivists" seeking to disrupt elections, and even nation-states applying offensive cyberwarfare capabilities [31]. Alex Halderman emphasizes that practically in every case where a fielded e-voting system has been publicly scrutinized by the capable independent security experts, it has been proved in the end to have serious vulnerabilities with the potential to disrupt elections, compromise results, or expose voters' secret ballots [15]. Technology adds more steps to the process, and in the same time increases the possibility of errors with each additional step, most of them are largely unseen by the voter [3]. We will not go into details to analyze all shortcomings of software engineering issues, such as code legacy, coding style, coding process, or code completeness and correctness, cyberwarfare capabilities, however we will summarize and describe general weaknesses associated with i-Voting.

4.2.1. Limited openness and understanding of the system for non-experts

Although nowadays modern technologies are widely applied in the realm of science, trade, business, or administration, when it comes to the implementation of IT technologies into voting processes, not just simple citizens, but even politicians, some experts, and scientists are still dubious [28].

4.2.2. Lack of transparency

The confidence in fair electoral process is based on the premises that all aspects of the elections process are directly observable [10] by the candidates, official observers, and people themselves; however in the remote i-Voting this is not the case. In fact, the voters, candidates and even officials do not really know how the voting system and software operates, and only a small group of specialists (such as system administrators) and other experts have the notion of the technical aspects of voting and manner of vote counting. Democracy functions well when the electorate has confidence that their vote matters.

Transparency has been a source of controversies, and core consideration since i-Voting inception. Fortunately, in 2004 the Committee of Ministers of the Council of Europe adopted Recommendation Rec (2004)11 on legal, operational and technical standards for e-voting, providing concrete guidelines that clarifies the issues related to the transparency [31]. In 2017 these standards were updated by Recommendation CM/Rec (2017)5, to ensure that electronic voting complies with principles of democratic elections in the context of present challenges and are the only existing international standards on e-voting so far [32].

Recommendation CM/Rec (2017)5 provides that the state shall be transparent in all aspect of e-voting [32]. This standard implies that the competent electoral authorities shall publish an official

list of the software used in an e-election (or at the very least it should indicate the software that will be used, the version, date of installation and a brief description). Also, it is recommended that voters should have access „well in advance"[13] of the election period to the components of the e-voting system and relevant information, in particular to documentation, source code and non-disclosure agreements [32]. Some experts consider as a good practice to publish code with a license restricting its use to code inspection or testing, providing transparency to i-Voting process [34], however it is worth understanding that code publication does not provide a guarantee of the security of the system, therefore is a trade off of security for transparency.

Voters are familiar with traditional voting methods that are well tried and tested, however a new voting system may cause concerns of different kinds. In order to promote understanding and confidence in any new i-Voting system, including in its transparency, voters shall be informed in clear and simple language, about: a) any steps a voter may have to take in order to participate and vote; b) the correct use and functioning of an e-voting system; c) the e-voting timetable, including all stages [31,32]. It is very important for voters, especially for those who are not familiar with i-Voting system and for elders, to have opportunity to practice the moment of casting their vote.

Auditing, observation, and monitoring of the election process not only enhance transparency, but also provide additional confidence for voters. Assessment that i-Voting systems function correctly and the security is provided is essential, therefore the system as a whole shall be disclosed for an independent evaluation and certification purposes [32]. The electorate must have the confidence that the election process is fair and the process is transparent, the system software must be open for inspection and the „design, implementation, development practice, operational procedures, and testing procedures must all be unambiguously and consistently documented" [3].

4.2.3. Risk of manipulation by insiders with privileged access to the system

One of the most important aspects of system security is the personnel who will use it. Much effort is invested in securing the system from external threats, as the developers and administrators of the system are often assumed to be harmless [3]. However, it should not be excluded the possibility of fraud through large-scale manipulation by a small group of insiders. In the opinion of Newman more often than not, the truly damaging attacks come from within [29]. Therefore the people involved in developing, operating, and administering i-Voting systems must be of unquestioned integrity.

4.2.4. Malicious Software Programming

The risk that programmers will try to rig elections through misleading software has led to specific processes and policies to avoid such deceptive event. Software code passes through numerous internal and external checks, including rigorous certification testing by independent certification bodies before use in an actual election [6].

Some experts consider that because the voting system software is engineered months in advance of actual elections, it is very unlikely for programmers to know the candidates for elections and to

[13] The expression „well in advance" is defined in the Guidelines for the implementation of transparency and observation recommendations as clear time frames that are set in national regulations for such disclosure and that the planned deadlines allow stakeholders to exercise their rights, react to such disclosures, and request changes. In order to respect the "well in advance" criteria, experts recommend twelve months before the Election Day for disclosure of information.

know how their names will appear on the ballots [1, 3]. However we can claim that testing e-voting systems for different security problems, especially if they were intentionally introduced and concealed, is basically impossible. Thus there is a high possibility to insert by programmers obscure combinations of commands and keystrokes that will slip through quality assurance testing. A double or even triple checking is never unnecessary. Also, it could be a possibility that voter's personal computers are virus/malware-infected which, in turn, can result in distorting the vote decision or/and affect the whole system of i-Voting.

4.2.5. Vulnerability to hacking

If there is no external communications pathway, then there is no risk of hacking, or gaining unauthorized entry into the system, however all the processes, including transmission of the election results, are performed via the Internet. An attacker who strikes early enough can introduce malicious code into the counting server by using a chain of infections that parallels the configuration process [15], especially if encryption and verification are not sufficient. It is reasonable to assume that the systems will be exposed to higher numbers of attempted attacks and manipulation as the use of e-voting becomes more widespread.

For some scholars i-Voting is a gamble with democracy, as there is not enough confidence in cyber security. An independent evaluation of e-Voting system in Estonia shows how shockingly easy it can be hacked and defrauded [33]. Evaluation was based on election observation, code review, and laboratory testing, and revealed staggering gaps in procedural and operational security. It was proved that the system architecture that leaves it opened to cyberattacks from foreign powers could alter votes or leave election outcomes in dispute. Experts confirmed that results were so alarming that they urgently recommend that Estonia discontinue use of the system [33]. We should not forget that Moldova is also situated as Estonia in the area of Russian interest; therefore it is a high possibility of hacking as was in the case of Estonia in 2007. Experts consider that attacks on i-Voting systems can be launched by anyone in the world, and in many cases may be successful while remaining completely undetected, consequently, this type of voting, in general, cannot be made completely secured for use in real elections for the foreseeable future [20]. The attack could be operated by a foreign country, candidate or party who wants to win the election at any cost, or even a hacker who just wants to prove his skills by disrupting the elections.

The threats on i-Voting security could be diverse and mainly refers to: a) denial of service, when hackers may compromise the availability to a voting system, such as „Ping of Death" or „Packet Flooding"; b) viruses aiming at destroying e-voting systems; c) worms that are viruses that do not change any existing program or file to spread itself; d) Trojan horses, that can delete or modify important files from the computer, by planting a harmful virus, or even stealing user's passwords etc.[1]

4.2.6. Increased infrastructure and environmental requirements

The Republic of Moldova consolidates its position in international rankings regarding the speed of the Internet. According to the study of Netindex, Moldova is on the 6th place at download and upload speed with 40.6 Mbps and 60 Mbps [27]. The country ranks 3rd in the world by gigabit coverage with around 90% of the population having the option to subscribe to a gigabit plan [27]. However we need to take into account issues related to constant power supply, communication technology, the possibility of system attack or breakdown, or connection failure, for instance in case of bad meteorological conditions or accidents.

4.2.7. Danger of interference in uncontrolled environment

E-voting in uncontrolled environments happens without any supervision and cannot be controlled by the election administration. This can be done from home, on the voter's personal computer, or potentially anywhere on mobile or public devices. With voting in uncontrolled environments, concerns regarding the danger of interference by someone else in proximity to a voter (at home or work) in order to control the voting decisions could be really high. Family voting, intimidation, vote-buying, fraud, forcing to vote selling, as well as the technical integrity of the device from which the votes are cast, all need specific consideration. Current forms of i-Voting have not yet been able to provide a definitive solution to such concerns.

4.2.8. „Digital divided" society

In opinion of some experts remote i-Voting has potential for a „digital divide" society, which can occur in two ways [10]. First case is a digital divide between those who have home computers with Internet connections and those who do not. Second situation is a gap between those who have faster access and those who have slower connections, hence lower quality access. In Moldova access is often less expensive and of higher quality in urban areas as customers can choose between a range of Internet providers, but those from urban area have mainly one choice – Moldtelecom – a national company. Those with lower income and who live in rural areas are at a disadvantage if they cannot afford it. Also, seniors in Moldova have very low rates of technology adoption than the general public; this group is more digitally disconnected than others and also mainly because of the low income. Therefore the extension of i-Voting has the potential to result in emerging of a „digital gap"[30], to create divides with respect to many socioeconomic variables, such as income, age, education, gender, geography etc.

4.2.9. The need for additional voter education campaigns

Implementation of i-Voting requires a voter education campaign to ensure that the public is aware that i-Voting is an option, and voters are able to understand and use the on-line system to cast a ballot. It is recommended to prepare a series of educational videos and make them available on social networks to explain what i-Voting is, how it works, and its benefits. Without correct marketing and advertising it will be difficult to engage electors.

The lack of adequate voters' technical skills to use the remote i-Voting could be also a problem, thus an additional campaign has to be organized for citizens who have never used a computer before, or did not have opportunity to use it frequently, such as low income citizens or seniors. Still, there is a notable digital divide between younger and older Moldovans, as many seniors, less affluent or with lower levels of educational attainment continue to have a distant relationship with digital technology.

5. Conclusions

Electoral authorities and the Parliament of the Republic of Moldova are in the process to adjust the legal and regulatory framework to allow the implementation of i-Voting system. A non-binding i-Voting Pilot will be conducted on a pre-selected group of voters within the country and from the Diaspora at the parliamentary elections in 2018. The Pilot should offer all technical, operational, and security features, as if it is used for legally binding elections (except the legal validity of the results is

not checked), and aim not only to test the security and reliability of the system, but also to gather valuable feedback from experts and society.

Taking into account all circumstances, such as legal environment, demographic situation, ICT development, social demand and political consensus, we can conclude that Moldova is ready to implement e-voting (i-Voting) system. However a range of potential shortcomings analyzed in the paper points very clearly that i-Voting cannot be offered as an exclusive voting method, but as an auxiliary voting channel to the traditional voting system. Hence, it remains essential that voters are given the possibility to participate using traditional methods. In this context, it is advised for a step-by-step approach to i-Voting process, with necessary trials and gradual implementation of the system. As a dimension of e-government or e-democracy, i-Voting can be seen as a critical infrastructure of a democratic polity.

6. References

[1] AL-AMEEN, A., TALAB, S., The Technical Feasibility and Security of E-Voting, in: The International Arab Journal of Information Technology, vol. 10, no. 4 (2013).

[2] ANRCETI, The number of users accessing the mobile Internet based on 4G technology has exceeded the threshold of 500,000, http://www.anrceti.md/news25082017. Accessed on 12 December 2017.

[3] BLANKENSHIP, I.V., Trusting the Machine: Inherent Problems with Electronic Voting Systems, GIAC Security Essentials Certification (GSEC), February 2004.

[4] CEC, Election results 30 October 2016, http://www.cec.md/index.php?pag=news&id =1926&l=ro. Accessed on 12 December 2017.

[5] CONSTITUTION OF THE REPUBLIC OF MOLDOVA, 27 August 1994

[6] CRANE, R.E. et all., A Deeper Look: Rebutting Shamos on e-Voting, Verified Voting Foundation, May 2005, 1https://www.verifiedvoting.org/downloads/shamos-rebuttal.pdf. Accessed on 12 December 2017.

[7] DE ZWAAGER, N., SINTOV R., Driving Innovation in circular migration, Nexus Market Analysis, Chisinau, October 2014.

[8] ELECTION BC, A non-partisan office of legislature. Disscussion Paper: Internet Voting, August 2011.

[9] ELECTORAL CODE OF THE REPUBLIC OF MOLDOVA, Law no. 1381, 21 November 1997.

[10] ENGUEHARD, C., Transparency in Electronic Voting: the Great Challenge, Conference on „E-democracy - State of the art and future agenda", South Africa, January 2008

[11] GOODMAN, N. et all., A Comparative Assessment of Electronic Voting, Prepared for Elections Canada by Canada-Europe Transatlantic Dialogue, February 2010

[12] GOVERNMENTAL DECISION no.841 on the implementation of electronic identification document, 30 October 2013.

[13] GOVERNMENTAL DECISION no. 1090 on the integrated electronic service for authentication and access control (MPass), 31 December 2013.

[14] GOVERNMENTAL DECISION no. 405 on the governmental integrated electronic service for electronic signature (MSign), 2 June 2014.

[15] HALDERMAN, J. A., Practical Attacks on Real-world E-voting, in: F. Hao and P.Y. A. Ryan (ed.), Real-World Electronic Voting: Design, Analysis and Deployment, Auerbach Publications, New York, 2016.

[16] HDSATELIT, Number of subscribers to television, internet and telephony services in the Republic of Moldova, https://hdsatelit.blogspot.com/2017/06/numarul-de-abonati-la-servicii-de.html. Accessed on 12 December 2017.

[17] IDEA, Introducing electronic voting: Essential considerations, Policy Paper, December 2011.

[18] INTERNATIONAL TELECOMMUNICATION UNION, Moldova Profile, 2016, https://www.itu.int/net4/itu-d/icteye/CountryProfileReport.aspx?countryID=274. Accessed on 12 December 2017.

[19] INTERNET IN WORLD STATS, Internet on Europe Stats, http://www.internetworldstats.com/stats4.htm. Accessed on 12 December 2017.

[20] JEFFERSON, D.R. et al., A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), January 2004.

[21] LAW no. 467 on informatization and state information resources, 21 November 2003.

[22] LAW no. 71 on registers, 22 March 2007.

[23] LAW no. 101-XVI on the Concept of State Automated Information System „Elections", 15 May 2008.

[24] LAW no. 133 on personal data protection, 8 June 2011.

[25] LAW no. 91 on electronic signature and electronic document, 29 May 2014.

[26] MOLDOVA.ORG, Votul electronic o necesitate a moldovenilor de peste hotare, May 2012, http://www.moldova.org/votul-electronic-o-necesitate-a-moldovenilor-de-peste-hotare-230150-rom/. Accessed on 12 December 2017.

[27] MOLDOVA.ORG, Moldova, on 6th place in the world at Internet speed, 2014 http://www.moldova.org/en/moldova-on-6th-place-in-the-world-at-internet-speed/. Accessed on 12 December 2017.

[28] MUSIAŁ-KARG, M., Implementation of electronic voting and the matter of security, in: Annales Universitatis Maria Curie-Sklodowska, vol. XXII, Lublin (2015).

[29] NEUMAN, P. G., Security Criteria for Electronic Voting, September 1993. Available at: http://www.csl.sri.com/users/neumann/ncs93.html. Accessed on 12 December 2017.

[30] NORRIS P., Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide, Cambridge University Press, 2001.

[31] RECOMMENDATION Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, 30 September 2004.

[32] RECOMMENDATION CM/Rec(2017)5 of the Committee of Ministers to member states on standards for e-voting, 14 June 2017.

[33] SPRINGALL, D. et al., Security Analysis of the Estonian Internet Voting System, 2014, https://jhalderm.com/pub/papers/ivoting-ccs14.pdf. Accessed on 12 December 2017.

[34] UNDP, Feasibility Study on Internet Voting for the Central Electoral Commission of the Republic of Moldova, Report and Preliminary Roadmap, Chisinau, 2016.

Open Government Data in Hungary

Anna Orbán[1]

DOI: 10.24989/ocg.v331.31

Abstract

Today it is increasingly evident that data is the new determining element in the economy and society. Digital data is essential resources for economic growth, competitiveness, innovation, job creation and social development.

For well-founded decisions, real data containing all the necessary information are required. Public organizations are obliged to collect and store vast amounts of data. However, the question arises: who has access to them and for what purposes are they used for?

Open Data has become increasingly prevalent both on organizational and national levels. By making the datasets available to the public, institutions have become more transparent, efficient and more economical. There are EU and national strategies and programs to support open public administration by providing an appropriate legal environment and recommending practical measures.

Freedom of information guarantees the accessibility of public data. However, accessibility is blocked by several challenges and obstacles, such as traditional approaches, legal constraints, practical and technical problems.

The aim of this paper is to interpret the basic concepts of open government data, and present some of the problems of Hungarian data policy, legal regulations and practical implementations.

1. Data of public interest and/or open data

In Hungary, the protection of personal data and the publicity of data of public interest have been fundamental rights enshrined in the Constitution since 1989. „*Everyone shall have the right to the protection of his or her personal data, as well as to access and disseminate data of public interest*." [7, Sections 59 and 61.] [16, Article VI (2)][2]

The concepts of personal data and data of public interest have been present in Hungarian law for almost three decades, but their interpretation and practical application are still not uniform.

Personal data

"Personal data shall mean data relating to the data subject, […] as well as conclusions drawn from the data in regard to the data subject." [4, Section 2(1)] [3, Section 3(2)]

[1] National University of Public Services, 2 Ludovika sqr., H-1083 Budapest, Hungary, e-mail: orban.anna@uni-nke.hu

[2] All translations of Hungarian laws by the author.

The main rule is confidentiality and privacy. Personal data is protected and manageable only for specific purposes, including the exercise of a right and the fulfilment of obligations, with the right of informational self-determination ensured.

Data of public interest

"Data of public interest shall mean data, other than personal data, that are managed by a body or person performing central or local governmental tasks or other public tasks defined by law [...]" [4, Section 2(4)] [3, Section 3(5)]

The main rule is to ensure publicity, as well as the transparency of public finances and the management of national assets. The term does not include any privately held data of public interest. Data of public interest is not equivalent to Open Data, as access to the former can be restricted (e.g. classified data, business secrets, data required for decision making, restrictions motivated by defense or national security interests, etc.).

Data public on reasons of public interest (since 2004)

"Data public on reasons of public interest shall mean any data, other than public information, that are prescribed by law to be published, made available or otherwise disclosed for the benefit of the general public." [3, Section 3(6)]

Data public on reasons of public interest include certain personal data of individuals acting within the scope of responsibilities and authority of a body undertaking public duties, such as their name, function, job position, executive mandate and other personal data as defined by law.

Business data may also be public on reasons of the public interest, if businesses use public funds or state budgets, or have a contract with a state body or a local government.

2. Regulatory environment

The European Union (EU), the United Nations (UN), the Organization for Economic Co-operation and Development (OECD), the World Bank and other organizations have developed and issued many strategies, initiatives and documents to open up government data. Over the past decade, national governments have also developed their strategies and regulatory documents to manage and access public data.

In Hungary, data creation, data management, data usage and data provision appear in a number of laws. From the point of view of access to and use of public data, it is useful to take a closer look at some of them.

The constitutional amendment promulgated on October 23, 1989 created the constitution of the republic, which first raised the protection of personal data and freedom of information on constitutional level in Central and Eastern Europe. [7, Sections 59 and 61]

The Data Protection Act adopted after long preparations in 1992 was an up-to-date and European-styled law at that time.

The Act

- defined the notion of personal data, public interest data and later data public on grounds of public interest,
- ordered the protection of personal data,
- defined the rules for accessing public interest data,
- regulated the institution of data protection supervisor and data protection register,
- and finally its amendment adopted in 2003 ensured consistency with the European Parliament and Council Data Protection Directive 95/46/EC. [4]

When the PSI Directive (officially Directive 2003/98/EC [10]) entered into force, Hungary was not yet a full member of the European Union. After accession, the Hungarian government considered that the then constitution, regulation of data protection and electronic freedom of information fully complied with the EU acquis. Act XC of 2005 on the freedom of information provided for the electronic publication of data of public interest and the publication of legal and judicial decisions. [6] The 305/2005 (XII. 25.) government decree contained detailed rules for publication. [2]

The Council of Europe Convention on Access to Official Documents was signed by the Hungarian government in 2009 and ratified in 2010. With these moves, Hungary expressed its commitment to the democratic principle of transparency in state operations. The scope of the Convention is narrower than the scope of natural and legal entities to which the requirement of publicity of the data of public interest and, in particular, the right of access to official documents, is extended by Hungarian law.

In the latter, the definition of "public authorities" includes the following:

1. legislative bodies as regards their other activities,
2. judicial authorities as regards their other activities,
3. natural or legal persons insofar as they perform public functions or manage public funds, according to national law. [8]

After nearly two decades, in 2011, the old Data Protection Act was replaced by a new Privacy Act. The Privacy Act has a decisive role in the data ecosystem, with many other laws referring to it. When it was drafted, the provisions of the PSI Directive were known, but legal harmonization had not yet taken place.

The Act

- interprets the most important definitions,
- provides for the protection of personal data,
- defines the rules for access to data of public interest,

- requires disclosure of data of public interest, and the operation of the central electronic register of public information and the single data retrieval system,

- setting up a new data protection authority, the National Authority for Data Protection and Freedom of Information (NAIH) instead of the data protection supervisor, creating rules on the status and responsibilities of the authority. [3]

In 2012, the new Public Data Act (Act LXIII of 2012) has been aligned with the 2003 PSI Directive (with a delay of several years). The 2013 amendment to the PSI Directive (Directive 2013/37/EU [11]) implied new tasks. The amendments to the Privacy Act and the Public Data Act (Act XCVI of 2015) brought the relevant laws in line with the EU acquis. The Public Data Act currently complies with the PSI Directive.

The Act

- defines the principles for the reuse of public data,

- regulates the process of re-using, remuneration and format requirements,

- stipulates the conclusion of a reuse agreement,

- contains special rules for the reuse of cultural public information.[5]

Legal harmonization with the European General Union Data Protection Regulation (GDPR [12]) is a task for 2018. Although there are only a couple of months left until the May 25th, 2018 entering into force of the GDPR, there is only a draft amendment as per March 2018, still to be submitted to Parliament.

Hungarian public data are regulated by a fairly large number of laws whose relevance and consistency must be ensured. Over the past few years, the PSI Directive has been formally implemented, but the government still has to issue the executive orders and establish uniform and correct practices.

3. Access to public data

Public interest data are published on several levels:

- based on the obligation of publication by electronic means,

- based on data requests, such as

    - data requests of public interest,

    - data requests for statistical analyses or scientific research.

    - data requests under a public data reuse agreement.

General provisions on access to information of public interest shall not apply to the disclosure of information from official records that is subject to the provisions of a separate law.

3.1. Obligation of publication by electronic means

Access to public information whose publication is rendered mandatory under Act CXII of 2011 shall be made available through the internet, in digital format, to the general public without any restriction, in a manner not to allow the identification of specific individuals, in a format allowing for printing or copying without any loss or distortion of data, free of charge, covering also the functions of consultation, downloading, printing, copying and network transmission (hereinafter referred to as "electronic publication"). The range of data is defined by the publication lists (organizational and personal data, activity, operation data, and management data).

Access to data on the publication lists can be provided on a centralized website or on the organizations own websites and on the public data portal. These portals do not directly support the reuse of data. It is also a problem that most data are not machine-readable, cannot be queried en masse, are not available with open licenses, or in some cases their timeliness is questionable.

According to the Privacy Act, anyone has access to the public data issued by the public organizations obliged for that as well as to references to such data by using the Public Data Finder (http://kozadat.hu/kereso/). Although since 2008 all public bodies have been obliged to provide data, many of them have fulfilled this obligation only partially, if at all. The proportion of regular data providers is low.[3]

Further efforts are needed to open public data so that anyone can access them for personal or business purposes. Simple publishing data is not enough to make them useful. Citizens and businesses are not interested in the data themselves, but the services that are being implemented on that basis.

3.2. Access to public information upon request

The procedure is regulated by the Privacy Act (Sections 28-31).

Data of public interest and data public on grounds of public interest shall be made available to anyone upon a request presented verbally, in writing or by electronic means.

Access to data of public interest is hindered by several factors. The deadline for making the data available is 15 days. The body with public service functions that has the data of public interest on record is not obliged to comply with requests for public information if the requesting party does not provide his/her name, or a legal person fails to provide its name and contact details through which the requested dataset or any other information can be provided. This regulation eliminates the possibility of anonym data requests. Fulfilling a repeated data request for the same dataset by the same claimant within a year is not mandatory. The data used for decision making by a public service body are not public for ten years from the date of their creation. Such decisions may be rejected even after the decision has been made if the data concerned are used for substantiating further decisions. The Privacy Act also significantly expanded the scope of chargeable costs.

[3] Up to 6500 organizations have provided data on the kozadat.hu portal. On January 1, 2018, in the public repository, 2812 institutions could be searched for 153,098 records. [14]

In determining the chargeable fee, the following cost items can be taken into account:

- the cost of the data storage device containing the requested information,
- the costs of delivery of such device to the requesting party,
- if the fulfilment of the request for information requires the deployment of disproportionate workforce, the additional labor costs can also be charged.

The rules for determining reimbursement are still missing.

3.3. Data request for reuse

The procedure is regulated by the Public Data Act (Sections 10-18).

Applicants may initiate the procedure by submitting a written request. The request shall contain:

- an explicit declaration that the public data indicated are requested for reuse;
- the applicant's name, postal address (registered office), telephone number and e-mail address;
- an exact specification of the public data requested for reuse;
- the desired format of the public data requested for reuse, including an indication of the technical means and the method which the applicant intends to use;
- the required frequency, if recurrent access is requested.

The application may be rejected if the public data concerned cannot be made available for reuse, are not available at all and cannot be procured from another public body either. The public body shall conclude a reuse agreement with the applicant about releasing public sector information for reuse. A public body may charge a fee for making available for reuse the public sector information managed by it. The applicable fee shall not exceed the marginal cost of collecting, producing, processing and distributing the public data.

The rules for determining reimbursement are also missing here.

If a request is rejected, the applicant may appeal to the National Authority for Data Protection and Freedom of Information (NAIH) or opt for a court action.

4. Data policy

In 2012, Hungary joined the Open Government Partnership (OGP) initiative. One of the commitments assumed was to improve the publicity of data of public interest and data public on grounds of public interest in accordance with the principles of the Privacy Act. The progress report on Hungary established that a large majority of local governments failed to comply with the publicity obligation and the information published was often of bad quality and not searchable by IT means due to their format. In addition, there was a lack of real and meaningful cooperation

between the government and civil organizations, which eventually led to the exit of the Hungarian government from the OGP at the end of 2016. [15]

Before that move, under Government Decision 1310/2015. (V. 21.), a White Paper on National Data Policy was compiled that recommended both a national data policy strategy and concrete measures. [1]

This vision outlined in the White Paper fully complies with the goals specified by the National Infocommunication Strategy and the Public Administration and Public Service Development Strategy, as well as with the EU initiatives. Although Hungary has not formally adopted a national data policy, the latter's objectives will appear in the Digital Success Program 2.0 as part of the development of the digital state.

The policy of reuse of public sector data and the protection of national data assets would be an important dimension of the state's role within a digital ecosystem.

Based on NHIT's earlier White Paper, the public policy strategy, prepared in accordance with DJP 2.0, aims at jointly analyzing these two aspects, coordinating and balancing foreign best practices and Hungarian government efforts.

In order to substantiate the strategy, there is a need for

- creating a data cadaster in the public sector;
- developing a public sector data management model;
- evolving a concept of the use of public sector data assets;
- measuring organizational maturity related to the reuse of public sector data;
- compiling best practices abroad and home. [9, pp. 104.]

According to current plans, further research is required for drafting a strategy that covers both a national data policy and the reuse of public data, recommending legislation and measures to develop public administration. [9, pp. 102-105.]

5. Summary

Data are essential resources for economic growth, competitiveness, innovation, creation and society's progress in general. The aim of international organizations and individual states is to establish a well-functioning and efficient data ecosystem. Over the recent years Hungary has launched several data policy initiatives, but it still has no national data strategy. The publicity of public sector data is a fundamental right, but in practice, access to data and the utilization of data are hampered by a number of factors.

Some key concepts are not interpreted uniformly, with the Hungarian terms differing from definitions of the PSI directive. Instead of the concept of public sector information (PSI), Hungarian legislation usually applies the concepts of public data (data of public interest and data public on grounds of public interest).

Although the publicity and reuse of public data is provided by law, their practical application is difficult. There is no real open data portal for Hungary. The practice of requesting public data and data for reuse is not mature. The publicity of public interest data is a fundamental right, and the transparency of public sector operations and the spending of public funds should be guaranteed. Reusing typically involves large amounts of data, usually in a regular and profit-oriented manner. The detailed regulations of the data requirements have still to be elaborated.

To develop a well-functioning data ecosystem at national level, it is necessary to develop a unified government data strategy and then make well-considered measures. The White Paper is a good basis for this, as it integrates the principles of the production and utilization of national data assets, emphasizing the role of open data. Upon drafting a national data strategy, foreign and domestic good practices and initiatives by the European Union should be taken into account, in line with the PSI, INSPIRE and GDPR directives.

6. References

[1] 1310/2015 (V.21.) Government Decision on measures required for the wide-scale reuse of public sector information.

[2] 305/2005 (XII. 25.) Government decree on specific provisions relating to the electronic publication of Public Sector Information (PSI), the single PSI search service on inventory and data integration.

[3] Act CXII of 2011 on the right of informational self-determination and on freedom of information (Privacy Act).

[4] Act LXIII of 1992 on the Protection of Personal Data and the Publication of Data of Public Interest (Old Data Protection Act).

[5] Act LXIII of 2012 on the re-use of Public Sector Information.

[6] Act XC of 2005 on the freedom of information.

[7] Constitution of Hungary (the amendment proclaimed on 23 October 1989).

[8] Council of Europe. (2009). Council of Europe Convention on Access to Official Documents (CETS No.205). Tromsø. Retrieved 02 20, 2018, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205/signatures?p_auth=Y8QKEMS5

[9] *Digital Success Programme 2.0.* (2017). Budapest. Retrieved 02 20, 2018, from http://www.kormany.hu/download/6/6d/21000/DJP20%20Stratégiai%20Tanulmány.pdf

[10] European Commission. (2003). Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. *Official Journal of the European Union*, 90-96.

[11] European Commission. (2013). Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information. *Official Journal of the European Union*, 1-8.

[12] European Commission. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR). *Official Journal of the European Union*, 1-88.

[13] NHIT. (2016). *White Paper on National Data Policy.* Budapest: National Council for Telecommunications and Information Technology. Retrieved 12 28, 2017, from http://nhit.hu/dokumentum/175/Adatpolitikai_feher_konyv_2016081_EN_20161121.pdf

[14] NISZ (National Infocommunications Service Company). (2018, 01 01). *About*. Retrieved 01 10, 2018, from Public repository: http://kozadattar.hu/node/5

[15] OGP. (2017, 12 28). *Hungary (withdrawn)*. Retrieved 01 15, 2018, from Open Government Partnership: https://www.opengovpartnership.org/countries/hungary-withdrawn

[16] The Fundamental Law of Hungary (updated version of 1 July, 2016).

Cybersecurity II

IMPROVING DISTRIBUTED VULNERABILITY ASSESSMENT MODEL OF CYBERSECURITY

Kálmán Hadarics[1] and Ferenc Leitold[2]

DOI: 10.24989/ocg.v331.32

Abstract
In the digital age more and more services and data are available over the Internet. Companies and public organizations becoming increasingly vulnerable related to hacks and cyberattacks. In order to provide successful online services, effective security initiatives and targeted protections are necessary to mitigate security risks. Effective cybersecurity more than deploying firewalls and other security software (e.g. antivirus, intrusion detection/prevention systems.). Through risk assessment and risk management practices we can identify critical parts of information systems and can transform them into security tactics. Furthermore in the Distributed Vulnerability Assessment (DVA) model three factors are identified: (1) characteristics and prevalence of cyber-threats, (2) vulnerabilities of IT infrastructure and its components and processes, (3) vulnerabilities deriving from users' behavior.

In this paper, we examine and improve our mathematical model of Distributed Vulnerability Assessment. This model can be extended for using additional information and considerations. This paper also presents a practical method which can be applied to eGovernment infrastructure and services also to reduce the impact of malware attacks of the information system.

Keywords: *distributed vulnerability analysis, malware, threat, cybersecurity*

1. Introduction

The recent evolution of information technology caused significant increase in productivity and everyday life. These days using online services is self-evident. Our personal and other specific data are accessible from different devices like computers, tablets, smartphones and other IoT devices. However if our data are available online they are exposed to theft or unwanted manipulation. There are different cyber-threats. With the help of that cyber criminals can steal unauthorized data or other credential information. In the digital age the information security became a crucial point of an information system. If you want to launch a new digital service you have to ensure data security. An unwanted security incident can disrupt our business success, and partners will abandon our service.

If we want to observe the protection level of our IT system and infrastructure we have to consider our data flows and processes. But all systems, networks, applications or other infrastructure element may contain vulnerabilities or just misconfiguration. Newer and newer threats are appearing everyday therefore continuous review of security rules are expected. In order to achieve digital enterprise success, effective security initiatives and targeted protections are necessary to reduce or mitigate security risks.

[1] University of Dunaújváros, H-2400 Dunaújváros, Táncsics M. u. 1/A., hadarics@uniduna.hu
[2] Secudit Ltd., H-8200 Veszprém, Kupa utca 16., fleitold@secudit.com

As a result of our research we have define DVA (Distributed Vulnerability Assessment) model [1].

In this model three distinct but highly interactive sources of vulnerability are considered [2]:

(1) Characteristic and prevalence of harmful cyber-threats

(2) Vulnerabilities of the IT infrastructure and its processes;

(3) Vulnerabilities deriving from users' behavior.

More detailed information about the model is available in [1] and [2].

2. Background and related work

More and more organizations around the world perceived the need of risk assessment in order to enhance information security. Standard organizations e.g. NIST or ISO have published their risk management guides [3],[4]. These are attempts to create a common language and guidance for assessing and mitigating risks related to information security incidents. An information security incident can be a single or a sequence of unexpected or unwanted information security event. New vulnerabilities are discovered on average daily in different software and hardware devices. It makes possible launching new attacks or other types of exploitation.

An infrastructure is as secure as the weakest component in the system. "To succeed, a malware attack directed against a protected target network requires successful execution of the malicious code by the protected IT with sufficient authorized user facilitation to subvert network security." [5] Security metrics generally focus on malicious activity and protected IT. Metrics related to user behavior are less common. The DVA model focus on all of three main factor discussed earlier. Using different mathematical formulas and techniques the risk value for a threat can be estimated.

3. Limits of DVA model

A quantitative risk assessment model provides appropriate results if its input parameters are derived from some irrefutable facts. Certain factors have more impact on overall result. But adding new factors to the model can help to refining and clarifying the issue.

The DVA model has some limitations:

- The probabilities that are used in formulas need to be independent. Otherwise the estimation won't be accurate.
- Detailed unfolding of properties of model elements are necessary for reaching the expected accuracy.
- The model doesn't identify the direct connections between elements.

4. Alternative approach

The starting triangle is very similar to DVA model elements. In the first corner there are the Users. Users are humans, they can do something on computers (devices), and they have activities on IT infrastructure. The second main corner are the devices. They are just physical devices, they have hardware components and they are able to execute programs. The third main corner are the threats [6]. There could be a plenty of possible threat types [7] related to an attacker or any unwanted event that can be occurred.

The three main corners represent the corners of our triunal model, they are the main actors in any security issue.

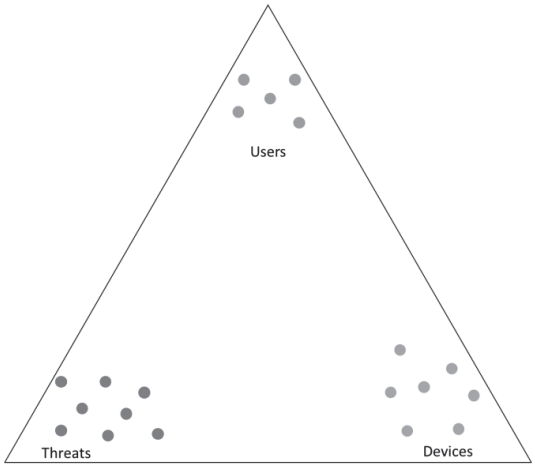

Figure 1: Main actors of the cybersecurity vulnerability assessment

A set of points inside the triangle contains the actors that have impact on information security and they belong together based on some attribute.

Beyond the main actors we can define other influential set of points. These are

- User tricks
- Credentials/access rights
- HW/SW elements
- Cloud services
- Vulnerabilities
- Protections.

In the model we can define connections between set of points. These connections generally link together points from different sets. Later we will define the exact meaning of a connection that is exists between different set of points. It can be said generally if there is connection in the pattern that belongs to a specific threat it carries a security hazard.

We have hardware and software elements as well. Of course two devices have different HW/SW elements, they can be similar. So this set of light green points represent different instances of HW/SW components. E.g. Windows 7 on device 1, Internet Explorer on device 2, Google Chrome on device 1, Microsoft Word on device 2. A line between a device and a HW/SW element indicates that the particular device has that component.

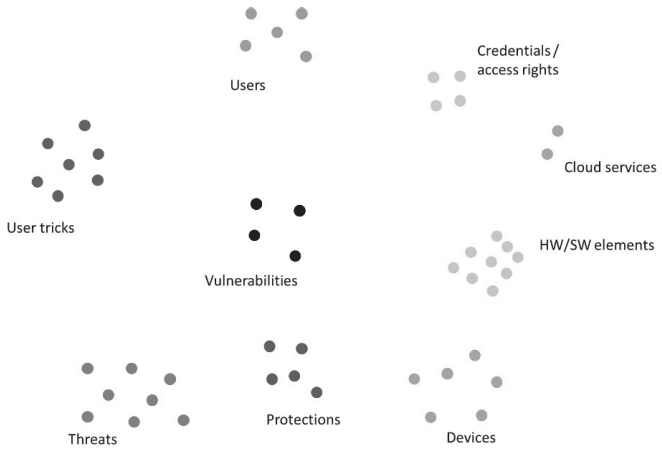

Figure 2: The influential actors of the cybersecurity vulnerability assessment

The next set of defined points are very similar to the HW/SW elements. They are cloud services. The cloud services can be assigned to the devices as well, if we define the connection between a device and a cloud service if the device is able to use the cloud service. E.g. if the Dropbox is installed or if there is an internet browser and the device has internet connection (in this case most of cloud services can work).

Users are the humans that use computers (devices). In fact they can access to one or more HW/SW components only. Now we assume that they do not make any physical changes in the machine. So they need credentials/access rights to HW/SW components and they may have credentials/access rights to one or more cloud services. So, a line between a user and a credential/access right indicate that the particular user has that credential/access right. And there could be a line between a credential/access right and a HW/SW element or a cloud service indicating which component can be accessed. Please note, that if a user has an administrator right to a computer then this user has credential/access right to all of its HW/SW components. But it can be limited by settings and/or policies. Users have their own behavior as they are humans. [8] There are user tricks that can be used by threats. The line between a user and a user trick indicates that there is a possibility that using the particular user trick the user will make what the threat requests/expects. The line between a threat and a user trick indicates that there is a possibility that the threat uses the particular user trick.

Each point in the protection group represents a SET of protections can protect a SET of HW/SW elements or cloud services. E.g. a firewall and an antivirus together.

A line between a threat and a protection indicates that there is a possibility that the protection does NOT block the particular threat.
A line between the protection and a HW/SW element or a point of cloud service indicates that the protection is installed to protect that HW/SW element or the cloud service.

There are vulnerabilities in the HW/SW elements and they can be in cloud services as well. Vulnerabilities are used by threats.

The line between a threat and a vulnerability means that the particular threat uses that vulnerability. The line between a vulnerability and a HW/SW element or a cloud service means that there is a possibility that the usage of the particular vulnerability against the HW/SW element or the cloud service is successful.

The line between a vulnerability and a credential/access right means that there is a possibility that the usage of the particular vulnerability against the credential/access right is successful. For example if the malicious activity tries to figure out the user name and the password.

In this model we represent a factor as a point of a set. With the help of defined connection we are able to find the concerning elements. We defined this representation the constellation model of vulnerability assessment.

5. Practical usage

The threat type is exploit. Exploits use vulnerabilities of HW/SW elements to execute their code on the device.

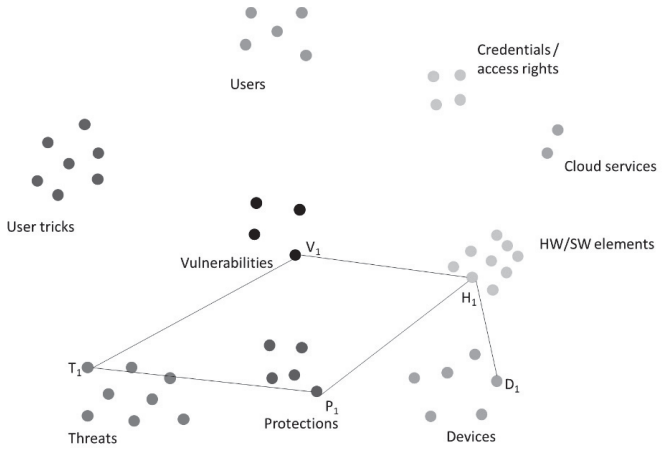

Figure 3: Representation of "Exploit" type threat

Successful operation requires the followings:

- Threat T_1 has to use vulnerability V_1.
- Vulnerability V_1 has to be related to HW/SW element H_1.
- For protecting operation of H_1, the P_1 set of protections (it can be empty set) exists and it is unable to block all of Threat T_1 executions against the HW/SW element H_1.
- And finally there should be the device D_1 which has the HW/SW element H_1.

Please note that all of the five lines indicates a probability or a relative frequency related to the operation.

T – V: How often use Threat T_1 the Vulnerability V_1.

V – H: How often successful the Vulnerability V_1 against HW/SW element H_1.

T – P: The blocking rate of threat T_1 by the protection (set) P_1.

P – H: The availability of Protection P_1.

H – D: How often the HW/SW element is working on device D_1.

In the next example the threat type is eavesdropping. During this an attacker attempts to obtain authentication information for a cloud service.

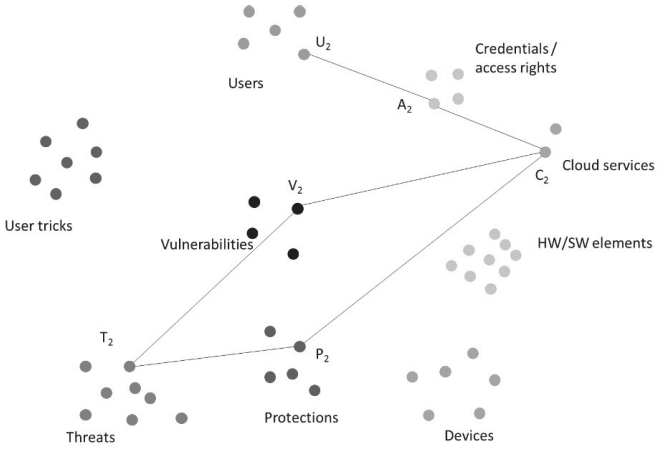

Figure 4: Representation of an Eavesdropping

Successful operation requires the followings:

- Threat T_2 has to use vulnerability V_2.
- Vulnerability V_2 has to be related to cloud service C_2.
- For protecting operation of C_2, the P_2 set of protections (it can be empty set) exists and it is unable to block all of Threat T_2 executions against the cloud service C_2.
- And finally there should be a user U_2 who has an access A_2 for cloud service C_2.

All of the six lines indicates a probability or a relative frequency related to the operation.

T – V: How often use Threat T_2 the Vulnerability V_2.

V – C: How often successful the Vulnerability V_2 against cloud service C_2.

T – P: The blocking rate of threat T_2 by the protection (set) P_2.

P – C: The availability of Protection P_2.

U – A: How often the User U_2 is using cloud service C_2.

A – C: How often the access rights A_2 are in use accessing cloud service C_2.

In the third example there is an e-mail client (H_3) which has a vulnerability (V_3). H_4 is the operating system which executes the attachment when the User (U_3) clicks. D3 is the device that executes H_3 and H_4. C_3 denotes the user's credentials to the e-mail client, C_4 to the used operating system. The applied User trick (scam) is represented by S_3. P_3 is the set of e-mail protections, P_4 is the set of endpoint protections.

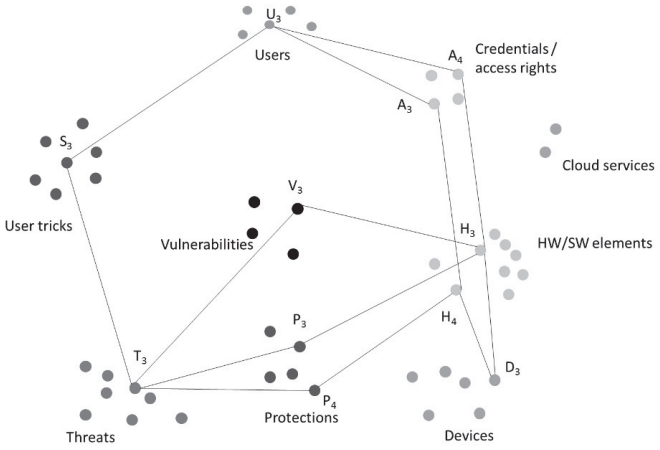

Figure 5: Representation of an e-mail related threat

All of the fourteen lines indicates a probability or a relative frequency related to the operation.

T – V: How often use Threat T_3 the Vulnerability V_3.

T – P: The blocking rate of threat T_2 by the protection (set) P_3 and P_4.

T – S: How often use Threat T_3 the User trick S_3.

S – U: How often user U_3 can be deceived by user trick S_3.

U – A: How often the User U_3 use the access to A_3 and A_4.

A – H: How often the access rights A_3 and A_4 are used to access HW/SW elements H_3 and H_4.

P – H: The availability of Protection P_3 and P_4.

H – D: How often the HW/SW element is working on device D_3.

6. Conclusion

In this paper we demonstrate our improved model of cybersecurity vulnerability. All important aspect of cybersecurity vulnerability are considered. There are a lot of possible threat types. If we put the actors onto the table, all of threat types can be characterized using the “connection graph”. If all of the influencers are drawn, then these factors influence the vulnerability of the single threat on a single device using a single user.

7. References

[1] HADARICS, K., K. Győrffy, B. Nagy, L. Bognár. A. Arrott. F. Leitold (2017): Mathematical Model of Distributed Vulnerability Assessment, 9th International Scientific Conference, Security and Protection of Information, 2017, Brno, Czech Republic

[2] LEITOLD, F., A. Arrott, K. Hadarics: Quantifying cyber-threat vulnerability by combining threat intelligence, IT infrastructure weakness, and user susceptibility 24th Annual EICAR Conference, Nuremberg, Germany, 2016

[3] International Organization for Standardization (ISO), ISO/IEC 27005: Information technology – Security techniques – Information security risk management (2008)

[4] National Institute of Standards and Technology (NIST), Special Publication 800-30r1: Guide for Conducting Risk Assessments (2012), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[5] LEITOLD, F., A. Arrott, and K. Hadarics, "Automating visibility into user behavior vulnerabilities to malware attack" Proceedings of the 26th Virus Bulletin International Conference (VB2016), pp. 16-24, Denver, USA, 2016.

[6] ENISA: Ad-hoc & sensor networking for M2M Communications - Threat Landscape and Good Practice Guide 2017 https://www.enisa.europa.eu/publications/m2m-communications-threat-landscape/at_download/fullReport

[7] VAVOULAS, N., Xenakis C. (2011) A Quantitative Risk Analysis Approach for Deliberate Threats. In: Xenakis C., Wolthusen S. (eds) Critical Information Infrastructures Security. CRITIS 2010. Lecture Notes in Computer Science, vol 6712. Springer, Berlin, Heidelberg

[8] ONWUBIKO, C. (2016) Understanding Cyber Situation Awareness, *International Journal on Cyber Situational Awareness*

[9] LEITOLD, F. and Hadarics, K., "Measuring security risk in the cloud-enabled enterprise." Malicious and Unwanted Software (MALWARE), 7th International Conference on Malicious and Unwanted Software, pp: 62-66, ISBN: 978-1-4673-4880-5. 2012.

OTT REGULATION A WAY OF COMBATING CYBERCRIMES

Veronica Mocanu[1]

DOI: 10.24989/ocg.v331.33

Abstract

In the past decade we have witnessed a rapid expansion of the Internet gadgets, Internet services and internet applications. This revolutionary communication network has significantly changed the way people live, communicate, and conduct business. However, from legal perspective all of these new challenges remain under covered, things that frequently could generate harm, abuses and cybercrimes. Therefore, by this research, it is proposed to discuss the main risks, which are generated by using of uncontrolled OTT and present perspectives of regulations. The article includes topics such as description of OTT regulations practices used for the moment, problems generated by chaotic regulations of OTT, perspective that we have to take, need for licensing and certification of new internet applications and services, setting of quality standards, and proposes for involvement in development.

1. Introduction

In the last 30 years, contemporary societies are involved in a continuous activity of developing and promoting the use of information technologies. There are intensively promoted actions of digitization and automation of human activity in such a way that human existence to be maximized. As a result, we find that efforts are not in vain, and the living conditions really have changed. If, 30 years ago, using the smartphones or remote control devices seemed utopian, today these are an indispensable part of human activity.

Moreover, not only living conditions, but also the forms of perception of reality and business development are changing. Today if you need a product you no longer have to go to the store, the product can be purchased online; if you prepare a bachelor thesis and you want to get informed, the internet is the most used way of documentation, here you can find last-minute news as well as information dating back to the previous centuries; if you want to go for vacation but you do not know which destination to choose, the internet gives you the description of the route, the hotel tour, pictures in online mode and even the real impressions of the tourists.

Through its existence, the Internet is changing the concepts, ways of existence, and the practices established for centuries.

Under the conditions of a digitalized life, digital information and communication have turned into indisputable values of contemporary human activity. Thus, through the possibilities, platforms and fields of activity available online, the Internet has been resized and it should no longer be interpreted only as a connection tool, it is to be regarded as a new medium of activity, the existence of which is determined by the technological conditions, human will, but also the legal framework.

[1] State University of Moldova, Law Faculty, Department of Public Law, Chisinau (Moldova), http://usm.md/

The on-line activity is not a virtual activity anymore, online activity has been significantly resized over the last few years, so that online activity is a real activity that produces real effects.

Thus, by this article, contrary to the replies that promote the idea of an unregulated Internet, we call for the regulation of the online domain, indicating that it is absolutely necessary, or only by regulation can be ensured a free, fair and equal environment for all subjects involved in use of the internet. We draw attention, however, that new regulations are to be developed only for new realities, and in other cases, the generally accepted rules can be applied by analogy.

As indicated above, the on-line domain is a multidimensional domain involving the activity of different actors in different areas. By this article, however, we propose to focus on researching the field of OTT, as a contemporary challenge of the information society today.

2. What are OTTs?

The concept of Over-The-Top (OTT) services has appeared in the audiovisual sector in the 2010s' to refer to the new market that was emerging alongside the traditional markets of television (hertzian, satellite and cable television) that included new forms of delivering audio and other media content over the Internet. Today, this concept commonly refers to the provision of content and applications, including communications services over the Internet (e.g. voice services, hosting services, email services instant messaging, web-based content (news sites, social media, etc.), search engines, and video and multimedia content, etc). Usual examples of such services are WhatsApp for text messaging, Skype for video chat and voice call services, YouTube for video content sharing, Netflix and HBO for video streaming services, Spotify and Deezer for music streaming services, etc. [7].

Even though we already have at worldwide level different regulatory practices, at European level, we do not have yet an official position regard official concept, classification and regulation of the new OTT services so far, but generally, opinions are divided into three camps. The representatives of telecommunications companies, being affected by the appearance of new services, put forward arguments for awarding the OTT to the category of electronic communications services and applying for them the same rules as for electronic communications providers. Technicians and developers largely award the OTT to the information society services category, indicating that these services can be applied by analogy to the E-Commerce Directive. More and more are those who advocate the idea of appearance of a distinct form of services to which specific rules are to be applied, and OTTs are to be considered as distinct forms of communication.

The term of OTT came about as a result of more traditional telecom services coming under competition from content and service providers offering similar solutions using web services methods [6].

Wikipedia explains that "… over-the-top content (OTT) refers to delivery of audio, video, and other media over the Internet without the involvement of a [network] operator in the control or distribution of the content. The Internet provider may be aware of the contents of the Internet Protocol packets but is not responsible for, nor able to control, the viewing abilities, copyrights, and/or other redistribution of the content. This model contrasts with the purchasing or rental of video or audio content from an Internet service provider (ISP), such as pay television video on demand or an IPTV video service ..." [12].

Being aware of legislative gap, preparing a study regard OTT players, European Parliament mentioned that it makes clear that an OTT service is not a transmission network, but is instead a service that runs over an Internet network; moreover, the OTT service provider is typically distinct from the operator of the underlying network. From European Parliament's perspective an over-the-top (OTT) service is an online service that can be regarded as potentially substituting for traditional telecommunications and audiovisual services such as voice telephony, SMS and television [13].

In order to advance some clarifications for the moment, designing in January 2016 a report regard OTT services, the Body of European Regulators of Electronic Communications ("BEREC") defines OTT as "content, a service or an application that is provided to the end user over the open internet" and introduce notion of CAPs in sense of presenting the new category of internet players - content and applications providers [2]. Including in the definition that what is provided can be either content, a service or an application, means that anything provided over the open Internet is an OTT service. This provision generally occurs without involvement of the IAP in the control or distribution of the service. Because the service is provided over the Internet this definition implies that OTT refers to content that usually arrives from a third party (OTT provider), not being provided by the IAP to which the end user is connected. However, it is also possible the IAP offers its own OTT services or partners with OTT providers [2].

BEREC emphasizes that the definition of OTT does not have a legal status: OTT is not a term that has a meaning in the ECN/S Framework. OTT services do however have relevance in debate on the new ECN/S Framework.

Taking in consideration the above mentioned definitions, we will retain that for the moment, OTT refer in general to Internet-based content, applications and services that ride "over the top" of networks and are accessed by end users through a broadband Internet connection without the direct involvement of a network operator or Internet Service Provider.

However, in sense of preventing any misunderstanding, we find that OTT providers point that frequently, over-the-top term is wrongly used in the telecom world to describe any unmanaged service delivered over IP (online services). Opposite to the BEREC position, they promote to use "over the top" notion just to describe any content, services, or applications provided over an infrastructure that is not under the administrative control of the content or service provider. Thus, if an operator offers an IP service (say IPTV), and that service is delivered over the operator's infrastructure (whether mobile, fixed, or otherwise), it should not considered as OTT. However, if that same operator, after building a content/service model, extends the service to any IP end point on another operator's network, then it becomes OTT. Whether the operator decides to use QoS for the service is irrelevant in the definition of OTT. In other words, OTT providers promote the idea that an operator offering a service to its own subscribers could not be considered as an OTT player; rather if quality and bandwidth will be enforced, from OTT provider's opinion, the mentioned service will be considered just as a managed ECS[2], and if not, it will be qualified as an unmanaged ECS service (online services). Only if it is extended beyond the boundaries of that telecommunication's infrastructure is will be correctly referred to an OTT service or player [6].

[2] Providing managed ECS refers to providers which offering the service has control over the fixed or mobile access network used for its distribution. The provider is able to use this control to dimension the network, and in many cases to reserve network capacity to guarantee the quality of the service. Thus, managed services are strongly linked to the underlying network. Examples of such managed services are fixed and mobile telephony and the IPTV service offered by many network operators.

Personally, I accept the phenomenon of new internet realities linked to Internet-based content, applications and services provided, but I not agree with use of notion of OTT, and necessity of making differences between Internet-based content, applications and services provided by IP and Internet-based content, applications and services provided by third party. Analyzing the interpretation provided, seems that OTT term has been artificially introduced as a way to escape from the current legal framework, prevent assimilation with classic electronic communication providers and avoid the assumption of obligations.

I agree that Internet-based content, applications and services represent new realities and differ by classic electronic communication, but the accents has to be pointed not just on forms of delivery, and statue of the players, we also have to take in account the type of information administered by CAPs, risks involved in context of administration, users rights.

Revising the above mentioned, we had identify tree types of service providers which deal with similar business, but pretend to different levels of regulation, so we identified managed *electronic communication services providers*- the provider offering the service, has control over the fixed or mobile access network used for its distribution. The provider is able to use this control to dimension the network, and in many cases to reserve network capacity to guarantee the quality of the service. Thus, managed services are strongly linked to the underlying network. Examples of such managed services are fixed and mobile telephony and the IPTV service offered by many network operators; *online services providers* - providers who rely on the public Internet for at least parts of their distribution. The provider has little or no control over a part of the distribution network in particular the access networks. Well-known examples of online services are Skype and YouTube; and *OTT providers* - internet-based content, applications and services providers that ride “over the top” of networks and are accessed by end users through a broadband Internet connection without the direct involvement of a network operator or Internet Service Provider.

Taking into consideration the above mentioned, it is clear that the possibilities of ensuring the quality of services are different and that the operator has obligations prescribed by law to ensure the quality of the offered services, obligations to maintain confidentiality, neutrality and also interoperability, but to OTT providers are not prescribed for the time being such obligations, they specifying that to them can not even be prescribed such obligations because they have practically no technical possibilities.

The issue that appears is related to the content, and applications that allow entering not administered content. Thus, a question arises, would it be correct to distinguish the subjects involved in the online activity only after the way of operating the services, I refer in this respect to services / content / applications provided by the operator through his own network and services / content / applications over-the-top, that means through a foreign network? Or would it be appropriate, however, to differentiate the subjects also depending on the type of information being administered, the rights possible to be exercised, the risks involved?

In response to this question, we believe that in order to prevent confusions, the online subjects should be differentiated not only depending on how the content / applications / services are provided but also on the type of performed online activity. As a result, we could distinguish *content providers, application providers, service providers, internet providers,* etc., establishing separate obligations and rights for each category, in the same time pointing to the need to cumulate all rights and obligations derived from the subject`s status (player). Thus, if the operator is both an internet provider and an application provider, he shall assume both categories of rights and obligations.

We believe that by such an interpretation could be eliminated the inequality raised at the moment by internet operators, who are investing in infrastructure but whose services are declining. Similarly, this form of regulation would bring clarity about the legal status of each type of subject involved in online activity, stimulating growth and competitiveness.

3. Do Internet-based content, applications and services have to be regulated or not?

Regulation of internet is another complicate issue, and here we also have different opinions, tech field tray to argue that internet has to remain free, and there is no place for government rules, in opposite states try to demonstrate that unregulated Internet-based content, applications and services could present a danger. On European level, regulating authorities confirm the need for regulation and states that the existing regulatory framework does not apply to OTT per whole.

By, this article we will take the part of state, and will plead for regulation of Internet-based content, applications and services.

The lack of regulation leaves room for interpretation and maneuver, but at the same time it can transform the internet into a black hole that can generate the construction of a wrong world, built contrary to moral norms, common good and social interest, focusing only on business and material values.

Viral content, security and privacy issues, lack of quality services, dangerous applications and uncontrolled games, psychological manipulation, fake news, hate speech, copyright violations could be mentioned just as few of consequences, which could affect us in an unregulated environment. In such circumstances, I propose to think to some questions: Does unregulated Internet really mean the free Internet? Does the free Internet is really the bet? Does internet players have enough moral qualities to be able to oppose the new challenges? I think no, that's why I think that by establishing of clear rules, adoption of common standards and by introducing of control technics and authorities we could prevent the harm, and regulation of OTT could impose itself as a way of combating cybercrimes.

To be more convincing about the need to adopt regulatory rules for the OTT, I will outline just some of the potential impacts and risks that may arise because of the lack of regulation.

3.1. Security issues

A number of OTT communication solutions do not support encryption. This implies that attackers can easily eavesdrop into an OTT service (such as VoIP conversation and IM services). Since such applications rely on phone numbers, a lot of specialist explore the feasibility, automation, and scalability of phishing attacks that can be carried out by abusing a phone number. As result, it is demonstrated that the novel system takes a potential victim's phone number as an input, leverages information from applications like Truecaller and Facebook about the victim and his / her social network, checks the presence of phone number's owner (victim) on the attack channels (over-the-top or OTT messaging applications, voice, e-mail, or SMS), and finally targets the victim on the chosen channel. As a proof of concept, taking a random pool of 1.16 million phone numbers, was presented that social and spear phishing attacks can be launched against 51,409 and 180,000 users respectively. Furthermore, voice phishing or vishing attacks can be launched against 722,696 users. Also, found 91,487 highly attractive targets who can be attacked by crafting whaling attacks.

Supplementary, was established that social (69.2%) and spear (54.3%) phishing attacks are more successful than non-targeted phishing attacks (35.5%) on OTT messaging applications. Although similar results were found for other mediums like e-mail, was demonstrated that due to the significantly increased user engagement via new communication applications and the ease with which phone numbers allow collection of information necessary for these attacks, there is a clear need for better protection of OTT messaging applications and development of new regulations .

3.2. Over-The-Top (OTT) bypass fraud

Over-The-Top (OTT) bypass fraud, a recent form of interconnect telecom fraud. In OTT bypass, a normal phone call is diverted over IP to a voice chat application on a smartphone, instead of being terminated over the normal telecom infrastructure. This rerouting (or hijack) is performed by an international transit operator in coordination with the OTT service provider, but without explicit authorization from the caller, callee and their operators. By doing so, they collect a large share of the call charge and induce a significant loss of revenue to the bypassed operators. Moreover, this practice degrades the quality of service without providing any benefits for the users [15].

By, this article, we state that OTT bypass is illegal. Firstly, a call to a certain phone number has to be routed to the operator to which the phone number was allocated by International Telecommunication Union (ITU) or national regulators. This is violated by OTT bypass, because the call is routed to the OTT provider instead. Moreover, most countries impose regulatory fees and taxes for incoming international calls. These are paid by the caller, but hijacked by the bypassing operator. Service level agreements between operators are also violated when an operator pays for a premium quality call route, but its calls are bypassed over the OTT network. Unlike many OTT services, OTT bypass has almost no benefits for the users. In practice, OTT bypass is similar (in its effects) to other types of interconnect bypass fraud, such as simbox bypass [16]. More than that, ITU recently created a working group to study OTT Bypass, where OTT bypass is clearly reported as a fraud [17].

3.3. Confidentiality of communications

Traffic analysis, used by OTT players could help in determining who is talking to whom. Such information can be beneficial to cyber criminals preparing an attack, e.g. for committing corporate espionage or personal attack [3].

3.4. Privacy risks

Some OTT services collect users' private information for commercial gains without making the customer fully aware of the exact details. There is also lack of thorough check on risk assessment and vulnerability levels of applications developed for the OTT market [3].

One issue that should concern all OTT users is the terms of service and end user agreements imposed by OTTs. A study shows that almost 70% of participants never pay attention to the terms of agreements and privacy policies while installing applications on their phones [18]. Moreover, it is impractical for users to read and understand the terms of service agreements of all the applications they are using. As a result, OTT users may unknowingly accept terms of use that come with the end user agreements or default application settings, that's why we think that bu providing common standards and regulations we can prevent appearance of privacy risks.

There are other vulnerability vectors such as use of application with tracking option on, which may pose a threat to national governments.

3.5. Internet manipulation

Internet manipulation may be conducted by internet based content, applications or services for purposes of propaganda, discretization, harming corporate or political competitors, improving personal or brand reputation or plain trolling among other things. To accomplish these objectives, online influencers, hired professionals and/or software − typically Internet bots such as social bots, votebots and clickbots − may be used [5].

3.6. Uncontrolled on-line games

Regardless of whether they are played on a mobile device, gaming console, or computer, video games have become somewhat of a daily ritual for many people. Unfortunately, not all people understand that online games can pose real risks to their personality, health, or social relationships. More and more opinions say that a prolonged and uncontrolled use of video games may cause gamers to experience serious psychological and physical effects including irritability, insomnia, sadness, anxiety, aggressiveness, depression, fatigue, loss of appetite, and discomfort [11]. Moreover, the daily victims confirm in the near future psychologists' predictions. Blue Whale Game, Roblox Game, My Friend Cayla Doll are just a few of the games that can be listed as fatal hazard games.

More than that, we have to take in account psychological construction of human being and as a consequence construction of internet environment. People tend to manipulated and attracted by forbidden things, so the internet is a parallel copy of the real world, not regulating, it can turn into dark area. Provided thesis, is confirmed not just from philosophical manner but also from psychological perspective, and last studies, mentioned more frequently, that content that evokes more anger or amusement is more likely to be shared, and this is driven by the level of activation it induces [9].

Providing real time, interactive Internet based content, applications and services for diverse players and environments is a great challenge for our time. We recognize that, in today's information environment, OTT plays a sizable role in facilitating communications, providing services and access content in our everyday life. In some circumstances, however, we recognize that the risk of malicious actors seeking to use Internet based content, applications and services to mislead people or otherwise promote inauthentic communications can be higher.

Information operations can affect the entire information ecosystem, from individual consumers of information and political parties to governments, civil society organizations, and media companies. An effective response, therefore, requires a whole-of-society approach that features collaboration on matters of security, education, governance, and media literacy [8].

As a consequence to the above mentioned, we could consider that together with technical development, regulation of OTT could impose itself as a way of combating cybercrimes.

4. What we have now on OTT regulations?

4.1. International Telecommunications Union (ITU) efforts

Recognizing the worldwide role of Internet based content, applications and services, the International Telecommunications Union (ITU) has initiated first steppes in providing general rules for OTT regulations. As result, in 2016 the study group appointed, adopted a communication encouraging governments to develop measures to strike an "effective balance" between OTT communications services and traditional communications services, in order to ensure a "level playing field" e.g., with respect to licensing, pricing and charging, universal service, quality of service, security and data protection, interconnection and interoperability, legal interception, taxation, and consumer protection.

They requested a fair level playing field and that OTT players has to be imposed as subject to the same regulations as those of the telecoms sector, when providing equivalent service.

In May 2017, ITU Council Working Group on International Internet-related Public Policy Issues (CWG-Internet) launched an open online and physical consultation on OTTs. The working group has evaluated opportunities and implications associated with OTT including policy and regulatory matters. It considers regulatory approaches for OTTs that ensure security, safety and privacy of the consumer and will work towards developing model partnership agreements for cooperation at the local and international level.

The physical consultation took place in September and received inputs from a wide range of stakeholders. During the World Telecommunications Development Conference (WTDC)—the main conference of the ITU's Development sector, ITU-D—which took place in Argentina during October 2017, several governments have sought to expand the ITU Internet public policy mandate. As we approach the ITU's 2018 Plenipotentiary Conference, or "Plenipot" we can expect conversations on regulatory frameworks to escalate in the ITU [10].

4.2. European Union's overview on OTT regulations

At European level, until now, we do not have a common understanding and unique regulation designed for OTT field. However, as part of its Digital Single Market Strategy, the European Commission is currently reviewing the EU telecoms framework. In September 2015, the Commission launched a public consultation, inviting stakeholders to submit their views on the existing rules and on possible alterations. As a tentative for clarification, BEREC present in 2015 a Report with regard to OTT services, by which provide some classification of OTT and provide some views regard potential future regulation. For the moment, BEREC refuse to accept completely, the idea that OTT present totally new realities, and they could not be assimilated to other services. There are for, they present a classification of OTT's, which was proposed to be put on the basis of future regulations. Having in mind the idea of equity and equal regulation, BEREC propose to distinguish OTT varieties as follow:

OTT-0: an OTT service that qualifies as an ECS;

OTT-1: an OTT service that is not an ECS but potentially competes with an ECS;

OTT-2: other OTT services.

However, more and more voices point that BEREC proposed taxonomy is already outdated and would create even more interpretation problems than the current obsolete ECS. The way forward is building upon IAS and ISS [4].

More than that confusion is generated by different national regulatory framework developed. At European level, certain types of OTT services are qualified, by national regulators, as (publicly available) ECS and, as such, are subject to regulation under current EU telecommunications laws. For example, in most (if not all) EU member states, Voice over IP (VoIP) services providing for a break-out to the public telephony network (PSTN) are considered regulated telecommunication services. BEREC qualifies these services as OTT-0. The OTT Report notes, however, that the scope of the ECS definition provided for in the Framework Directive (2002/21/EC) is not sufficiently clear. BEREC therefore suggests to clarify the definition of ECS to ensure that "it keeps pace with the current developments". BEREC also notes that the lack of clarity allowing for different interpretations of the ECS definition leads to a lack of harmonization between members states in assessing which OTT services constitute ECS. The classification as an ECS triggers the applicability of obligations such as emergency calling, safeguarding telecommunications secrecy, and telecommunications-specific consumer protection rules [1].

Unlike BEREC, the German Federal Network Agency holds the existing regulatory framework for ECS is yet applicable to certain types of OTT services. In the Cologne proceedings, the German regulator argued that Google is involved in the establishment of the connection and therefore responsible for the conveyance of signals.

More than that, Germany as well Russia, propose legislation that would require the owners social media companies networks and messengers to delete any “illegal content” within 24 hours, or they would face steep fines. In cases where the content isn’t clearly illegal, social networks can take up to a week to review a complaint. Social media companies face fines as high as $57 million if they do not comply with the new law.

In the media it is announced, that France is the next country which is ready to adopt a new social media law during the next period of time. In this circumstances, the European Commission could be force to take actions and go far with Internet based content, applications and services regulation.

4.3. Other OTT regulation practices

In August 2017, the Indonesian government via the Ministry of Communication and Informatics (MCI) unveiled a liability framework for OTT providers. The sweeping regulations cover a whole slew of companies including SMS and voice calls and email services, chatting and instant messaging platforms, financial and commercial transaction service providers, search engines, social network and online media delivery networks, and companies that store and mine online data. The regulation, which is currently under review, makes it mandatory for offshore businesses to establish a "permanent establishment" either through fixed local premises or by employing locals in their operations in Indonesia. Transnational companies are also required to have an agreement with an Indonesian network provider, and use local IP numbers and national payment gateways for their services [10].

Similar efforts to regulate online platforms are underway in Thailand. The National Broadcasting and Telecommunications Commission (NBTC) has committed to create a "level playing field" between OTT service providers and traditional broadcasting and telecommunications industries. In

April 2017, it suggested introducing bandwidth fees for online content providers, and has also proposed bringing OTT service providers under an operating license framework, taxing them for transactions by local merchants and making them liable for illegal content. In July 2017, the Thai government issued an ultimatum to OTT services to register with the national telecom regulator or face getting slapped with sanctions such as bans on advertising that would threaten revenue growth [10].

In Latin America, several countries including Uruguay, Costa Rica, Colombia, Argentina and Brazil are considering legislative changes to enable the taxing of OTT players. In Argentina, the government has issued a set of principles for telecommunications regulation that create obligations for registration of Internet intermediaries. Ahead of the Presidential elections in 2018 and with mounting opposition to his regime, the Zimbabwean President Robert Mugabe has created a Cyber Security, Threat Detection, and Mitigation Ministry to reign in threats emanating from social media. The government is also pressing ahead with a Computer and Cyber Crimes Bill, a comprehensive legislation that would allow the police to intercept data, seize electronic equipment and arrest people on loosely defined charges of "insurgency" and "terrorism" [10].

5. Future developments

Information presented above shows that regulation of internet based content, applications and services present itself as an actual discussion with many questions but few answers. However, we have many opinions evoked, we do not have a clear picture of internet-based content, applications and services which we have to regulate. For the moment, we have a huge variety of services and applications and forms of content providing (voice services, hosting services, email services instant messaging, web-based content, news sites, social media, search engines, video and multimedia content) but we do not have a common understanding of classification and assimilation of them. In such a way, clear identification of the content, applications, and services we intend to regulate must be set as a priority in the succession of the actions we are proposing to make.

Is clear that OTT services are new realities, which will affect our future existence, and work, that is why to build a future in old soul, I think is a wrong way, is better to create something new, which will work for future than just to adapt something that will be a solution for the moment. We should promote new regulations, which will be designed special for new realities and then to adapt it to new challenges in case if they will appear during the time. More than that, we have to take in account that summing of all internet based content, applications and services in one big reality could imposed itself as an impossible exercise, grace to their variety, that's why when we think to new regulation we have to think to different internet players dealing with administration of different content, application and services. The regulations should take into account the type of service and the rights to be protected in a differentiated and specific way. Services offered by travel agencies, financial institutions, property rentals, or those providing alternative local transport considered as public services, should not be regulated in the same way. However, we have to create a common legal foundation for entire internet-based content, applications and services field by introducing general principles linked assurance of fundamental human rights, security and contribute to equal development of all internet players.

Not having a unique jurisdiction of internet, we have to concentrate our efforts by concentrating efforts of all stakeholders in the same direction regardless of country or authority. The new legislation should not separate the interests of the communications companies from those of the OTT, but has to be develop in a way, as by it to contribute to promotion of cooperation between all

internet players and do not affect the interests of users. However, self-regulation, standardization certification inclusive philological certification should be promoted at all levels, or they could prevent harms and assure wellbeing.

Concluding, we can certainly mention that for the moment we face new internet realities linked to Internet-based content, applications and services provided. We agree that, during the last period, our common understanding of internet was changed, and common construction of World Wide Web is destroyed, we have new realities, new players, new requirements and new challenges, and as a consequence we have to find new concepts, new rules and new control and cooperation forms and by this way to be able to combat new form of risks and infringements.

6. References

[1] BACKER, MCKENZIE, EU intends to regulate Over-the-Top ("OTT") services, Germany 2016. Available at: http://www.bakermckenzie.com/-/media/files/insight/publications/2016/03/eu-intends-to-regulate-over-the-top-ott-services/al_germany_regulateottservices_mar16.pdf?la=en[Accessed 14 Dec. 2017].

[2] BEREC, Report on OTT services, 2016.BoR (16)35. Available at: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services [Accessed 14 Dec. 2017].

[3] COMMONWEALTH TELECOMMUNICATIONS ORGANIZATION, Research Study, The Dynamics of Over-The-Top (OTT) Services, 2016. Available at: http://www.cto.int/media/CTOOTTStudyPaperFinal_ReviewedDraft04Oct2016.pdf [Accessed 14 Dec. 2017].

[4] ETNO Response to the Public Consultation on the draft BEREC Report on OTT services BoR (15) 142, 2015. Available at: https://etno.eu/datas/positions-papers/2015/Reflection-Documents/RD418%20-%20BEREC%20OTT%20services.pdf [Accessed 14 Dec. 2017].

[5] "Internet Manipulation." Wikipedia. Wikimedia Foundation, Available at: https://en.wikipedia.org/wiki/Internet_manipulation[Accessed 14 Dec. 2017].

[6] "Introduction to OTT", OTT Source. N.p., 22 Mar. 2013. Web. Available at: http://ottsource.com/ott-tutorials/introduction-to-ott/ [Accessed 14 Dec. 2017].

[7] PALLERO, J., JIT SINGH CHIMA R., Proposals for regulating internet apps and services: understanding the digital rights impact of the “Over-the-top”, 2017. Available at: https://www.accessnow.org/cms/assets/uploads/2017/08/Access_Now_OTT-position%E2%80%93paper.pdf [Accessed 14 Dec. 2017].

[8] WEEDON, J., NULAND, W., STAMOS A., Information Operations and Facebook, in: Information Operations and Facebook, 2017. Available at: https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf [Accessed 14 Dec. 2017].

[9] BERGER, J., MILKMAN, K. L., What Makes Online Content Viral? in: Journal of Marketing Research, 2012. Available at: http://jonahberger.com/wp-content/uploads/2013/02/ViralityB.pdf [Accessed 14 Dec. 2017].

[10] PANDAY, J., An Over-The-Top Approach to Internet Regulation in Developing Countries, in: 2017 revised draft OTT regulation (Indonesia), 2017. Available at: https://www.eff.org/deeplinks/2017/10/over-top-approach-internet-regulation-developing-countries [Accessed 14 Dec. 2017].

[11] LI, W., & ANTHONY, B. (In press), Internet and Video Game Addiction, in: Oxford Bibliographies in Social Work. Ed. Edward J. Mullen. New York: Oxford University Press.

[12] "Over-the-top Media Services", Wikipedia. Wikimedia Foundation. Available at: https://en.wikipedia.org/wiki/Over-the-top_media_services [Accessed 14 Dec. 2017].

[13] Policy Department A: Economic and Scientific policy, Over-the-Top players (OTTs), Directorate General for Internal Policies, European Parliament, 2015. PE 569.979.

[14] GUPTA, S., GUPTA, P., AHAMAD, M. and KUMARAGURU, P., Abusing phone numbers and cross-application features for crafting, targeted attacks, in CoRR, abs/1512.07330, 2015. Available at: https://arxiv.org/abs/1512.07330v1[Accessed 14 Dec. 2017].

[15] SAHIN, Merve, Over-The-Top Bypass: Study of a Recent Telephony Fraud. Available at: http://s3.eurecom.fr/docs/ccs16_sahin.pdf [Accessed 14 Dec. 2017].

[16] REAVES, B., SHERNAN, E., BATES, A., CARTER, H., and TRAYNOR, P., Blocking cellular interconnect bypass fraud at the network edge, in USENIX Security, 2015.

[17] ITU Study Group 3, Question 9/3. Ott bypass. International Telecommunication Union. Available at: https://www.itu.int/itu-t/workprog/wp item.aspx?isn=10892#TOP.

[18] CHIN, E., FELT, A. P., SEKAR, V., and WAGNER, D., Measuring user confidence in smartphone security and privacy, in SOUPS ’12, 2012.

.

ADVANCED BIOMETRIC ELECTRONIC SIGNATURE IN PRACTICE – LESSONS FOR THE PUBLIC ADMINISTRATION FROM A HUNGARIAN CASE STUDY

Péter Máté Erdősi[1]

DOI: 10.24989/ocg.v331.34

Abstract[2]
Signing documents is one of the most general requirements in our daily lives, including routines in Public Administration. After significant development of e-Administration, the question arose as to how the clients can sign documents electronically. The European Union legislated this question by the Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. This Regulation (henceforward: eIDAS) gives a technology-neutral and high-level framework for using electronic signatures in the EU, it refers several implementing acts and standards, records applicable concepts and definitions, and declares several obligations for all Member States. The Regulation does not contain strong provisions for advanced electronic signature, but it defines four requirements for it. All electronic signatures which fulfil these four requirements have to be considered as advanced electronic signatures. In most of the cases, creating an advanced signature is easier and more cost-effective than creating a qualified signature, therefore it may be an alternative solution for signing documents in Public Administration also. This paper intends to summarize the relating legal environment and it demonstrates an implemented solution of advanced biometric signature in the private sector. Finally, we discuss the technical conditions of the applicability of advanced biometric electronic signature in Public Administration by discovering similarities and differences of application and acceptability.

1. Legal background of advanced electronic signature

We found the ultimate answer to the question, whether human signature can be used for signing in Public Administration. It is "yes". But there were unknown methods and solutions to implement it. We needed further development and innovation for implementing biometric signatures which are able to fulfil all requirements of advanced electronic signature as required by eIDAS. Using new innovations in the private sector usually requires greater caution for reducing legal risks and business risks. Therefore, the legal background is essential in case of a novel innovation.

1.1. Advanced electronic signatures in and out of eIDAS

eIDAS improves cooperation in the internal market by a commonly used and enforced legislation. In most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State, because the national electronic identification schemes in their country are

[1] National University of Public Service, Institute of e-Government, 1118 Budapest, Ménesi út 5., erdosi.peter.kdi@office.uni-nke.hu
[2] This paper has been written with the support and within the framework of KÖFOP-2.1.2-VEKOP-15-2016-00001 Public Service Development for Establishing Good Governance: Digital Governance and Digital Government Research Program.

not recognized by others. Mutually recognized electronic identification will facilitate cross-border provision of numerous services in the internal market and enables businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities. One of the objectives of eIDAS is to remove existing barriers to cross-border use of electronic identification means used in the Member States to authenticate, for at least public services. The European Regulation should establish the principle that an electronic signature should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature. In the Member States, organizations currently use different formats of advanced electronic signatures to sign their documents electronically. It seems to be necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically.

Consequently, according to the eIDAS, only such solutions can be used across borders which are examined and accepted by affected Member States as it is defined by Articles 27 and 37 of eIDAS. If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public-sector body, that Member State shall recognize advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the appropriate implementing acts[3]. Although the Commission has already defined the reference formats of advanced electronic signatures or reference methods where alternative formats are used by an implementing act[4], the biometric references are still missing from these methods.

The eIDAS differentiates three levels of electronic signatures: normal, advanced and qualified. Electronic signature means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign (Article 3 (10)), advanced electronic signature means an electronic signature which meets the requirements set out in Article 26[5] ((Article 3 (11)) and qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures (Article 3 (12)). In the preamble of eIDAS, closed systems, background processes of Public Administration and contractual requirements are excluded from the scope. That is why we need to discuss the following questions. Many thanks to Balázs Kőnig for the long discussions of these legal questions.

- Question 1: What are the requirements for creating advanced electronic signature in connection with eIDAS? Creating advanced signature based on eIDAS is possible only with using public trust services. Definitions of eIDAS are not applicable in closed systems, agreements and background processes of the Public Administration.

[3] Article 27 (1) of eIDAS

[4] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognized by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[5] Article 26 contains four requirements: it is uniquely linked to the signatory, it is capable of identifying the signatory, it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

- Question 2: Is it possible to create advanced electronic signature based on eIDAS in closed systems and background processes of the Public Administration? It is not possible to create advanced electronic signature between participants of closed systems using only elements of closed systems. Closed systems, contracts and background processes of the Public Administration are excluded from the scope of eIDAS. If these solutions do not use publicly trusted services for signing, the creation of advanced electronic signature based on eIDAS will not be possible.

- Question 3: Is it conceivable to create advanced electronic signature based on eIDAS without a signing certificate? Advanced electronic signatures based on eIDAS require public trust services (for instance issuing certificate for the signatory), consequently it is unconceivable to create advanced electronic signature based on eIDAS without a signing certificate.

It should be noted that these signatures and seals may correspond to the European definition of the digital signature[6] which is not a legal term. The American definition of digital signature is similar but a bit different in the NIST standard[7] [10]. The European standard allows a data appended to a data unit, which can prove the source and integrity of the data unit, as digital signature, but the American standard considers only data resulted by asymmetric cryptography as digital signature. Consequently, there is a legal question whether electronic signatures created in a closed system fulfil all requirements of advanced electronic signatures may be named as advanced electronic signature based on eIDAS or not. It seems to be that eIDAS does not extend to any trust services providing in closed systems[8]. It results that definitions of eIDAS are not applicable in any closed systems, agreements and background processes of Public Administration, therefore creating advanced signatures in such systems is also impossible only with internal elements. It would be a very interesting side effect of eIDAS, requiring exclusion of definitions instead of services. But if it is correct, we need to find further legal solutions at national level.

1.2. Advanced electronic signature in Hungarian laws

Hungary adopted the 93/1999 European Electronic Signature Directive by the Act 35 of 2001 and it was replaced after eIDAS by the Act 222 of 2015 defining general rules of electronic administration and providing trust services in Hungary. This Act (henceforward: Eübszt.) extends eIDAS. Two important sections can be cited: advanced electronic signature is a signature as defined by Article 3 (11) of eIDAS[9] and where a law refers to an electronic signature or an electronically signed document, an electronic seal or electronic document with a seal shall also be understood unless otherwise specified[10]. These sections result in three important consequences. The first is the general applicability of the definitions. The scope of this national Act is not restricted. Although it intends to regulate trust services and electronic administration, the definitions can be applied to closed systems, contracts and background processes of Public Administration as well. The second is the

[6] Digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient (ETSI EN 319 411-1, p.10.)
[7] Digital Signature: An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection (NIST 800-63-3, p.45.)
[8] See Article 2 (2) of eIDAS: This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.
[9] See Eübszt. Section 1 (22)
[10] See Eübszt. Section 99 (2)

signatory unification. Where a Hungarian law refers to an electronic signature or an electronically signed document, it can be signed by both natural and legal persons notwithstanding signatures do not equal to seals but both can be realized as a digital signature. The third is the cross-border inadmissibility. If these signatures are based on national law, cross-border acceptability can be ensured only by the similar extensions of national laws in all Member States. This governance method was defined by the Electronic Signature Directive, but it was obsoleted and repealed by eIDAS. It results that only electronic signatures based on eIDAS should be applied by cross-border closed systems, agreements and background processes of Public Administration, if legal effect is mandatory, until acceptance of these signatures enters into force in all Member States.

What can Hungarian financial institutes do if they want to eliminate paper-based documents and want to use only digital documents? There is an obvious answer, digitization should be implemented. But all processes of financial institutes are legislated by laws, thus digitization shall comply with all related legal provisions. The most important Act is the Act 237 of 2013, which prescribes numerous rules for credit institutions and financial enterprises. There is a special provision for contracting in Section 279 (1) according to a financial institution, with the exception of a single payment order and the derogation provided for in paragraphs (1a) and section 285, may only conclude a contract for financial and supplementary financial services in written form, including electronic documents signed with at least advanced electronic signatures[11]. Consequently, paper-based documents can be omitted if clients and the financial institute are able to sign documents with at least advanced electronic signatures. For fulfilling this requirement, further legal questions shall to be discussed in order to prove that advanced electronic signatures can be created both on the basis of eIDAS or national laws in Hungary.

- Question 4: Are the scope of eIDAS and Eübszt. different? Yes, eIDAS pertains to public trust services and Eübszt. describes additional rules for electronic administration and trust services at national level.

- Question 5: Can the definition of advanced electronic signature defined by Eübszt. be applied in closed systems, agreements and background processes of Public Administration? Definitely. Since Eübszt. is a part of the national law and its scope is not restricted generally, these definitions can be applied to interpreting concepts used by other national laws.

- Question 6: What kind of definition can be used if a national law refers the advanced electronic signature? European Regulations and Acts shall be applied primarily and national law should be used secondarily if there are no restrictions or it is not forbidden. Requirements for advanced electronic signatures are the same even the EU Regulation or Hungarian national law are applied.

1.3. Biometric signature in Hungarian Law

Hungarian Act relating to governmental offices[12] was extended on 21-10-2016 with a new paragraph (20/J. §), which allows using biometric technology for Governmental Offices in capital and county from 01-01-2017. In Offices and in the Government Window, electronically captured electronic images and dynamic data of the customer's signature can be used for authentication tools

[11] Section 279 (1) of Hungarian Act No. 237 of 2013
[12] Hungarian Act CXXVI of 2010 on Government Offices in the Capital and the County as well as the amendments to the Act on the Establishment of Capital and County Government Offices, and Territorial Integration

of electronic documents. In case of implementing this service, the Governmental Offices appointed by a Government Decree shall develop and maintain a signature sample database containing the picture and other dynamic data of the signature (e.g. strength of pressure, speed of moving). This database may not contain other personal or biometric data in addition to the data required for the evaluation of signature samples. These data may be recorded only with the voluntary consent of the customer, clients shall not be obliged to use this authentication method. When a signature is created on a device regulated in accordance with this Act, only the conformity with the specimen can be verified and an electronic clause of the result shall be attached to the document. This clause shall to be issued by a certified system and the document identifier has to be included also. The clause may not contain any dynamic data of the signature or any sensitive personal data. The electronic document with the mentioned clause shall be considered a private document with full probative force. In this construction, the documents may contain only the picture of the client's signature. This signature should not be considered as advanced electronic signature according to the professional opinion of Hungarian Association for Electronic Signature [4]. In this public service, it is not necessary to fulfil requirements of advanced electronic signature, because the Governmental Offices are able to issue documents with the specified clause as private document with full probative force based on this statutory authorization. There is no more information about the implementation procedures of this provision at the moment of writing this paper.

2. A novel innovation – how to create advanced biometric electronic signatures in practice

2.1. Rationale

In the literature, numerous articles can be found, which addressed the problems of using biometric signatures. We should differentiate – as in eIDAS – the identification data from the signature data from legal aspect. Signature is a data which is connected to other data[13], identification is a process which uses data instead of connecting to other data[14]. Authentication is another process which enables the confirmation of a claimed identity of natural and legal persons or the origin and integrity of a data unit[15]. In the development of a signature, the method of connection seems to be the most important part beyond to identifying capability of the signatory. This part is missing from an authentication process, because only a matching result between the recorded and presented electronic data has to be confirmed or refused. The innovator company had to plan, develop and deploy such signature method which is capable to comply with the requirements of advanced electronic signature.

The customer is the OTP Bank Plc.[16] as the largest bank in Hungary by number of branches (about 350-400). The predecessor of OTP Bank called the National Savings Bank was established in 1949 as a nation-wide, state-owned, banking entity providing retail deposits and loans. OTP Bank's privatization began in 1995. As a result of public offers along with the introduction of the bank's shares into the Budapest Stock Exchange the state's ownership in the bank decreased to a single voting preference (golden) share. Currently the bank is characterized by dispersed ownership of

[13] See Article 3 (10) of eIDAS: 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
[14] See Article 3 (1) of eIDAS: 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
[15] See Article 3 (5) of eIDAS: 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
[16] For more information see https://www.otpbank.hu webpage.

mostly private and institutional (financial) investors. After the realization of its own privatization process, OTP Bank started its international expansion targeting countries in CEE region, which offers more economic growth potential. Today OTP Group provides financial solutions to nearly 15.1 million customers through nearly 1,400 branches, agent networks and state-of-the-art electronic channels.

National University of Public Administration in Hungary issued a report named "Good State Report 2017" [5], which is based on a representative research (Report on Good State Survey, 2017 [2]) and covered several topics including preferred channels in Hungarian Public Administration. Having regard to the fact that the bank owned by the State formerly, correlation between usage of channels in the banking affairs and Public Administration can be assumed. Proving this assumption goes beyond the scope of this paper. Nevertheless, Hungarian people prefer channels in Public Administration as can be shown by the following table:

personal	postal services	call center	online	other
61.8%	5.8%	17.8%	14.7%	2.8%

Table 1: Preferred channels in Hungarian Public Administration (based on [5:169]

The main goal of the bank was to develop and use an electronic solution instead of paper-based documents which can be as similar to the paper-based process as possible and which fulfils legal requirements. Banking contracts shall be signed only in written form or with advanced electronic signature in Hungary. The main focus was on the contracting procedure between the bank and the clients. Extension of the process to signing other transactions and orders in branches by the clients or to signing documents in other back-office procedures by the officers or managers were expectable. Signing a paper-based document does not require much knowledge and many devices from the clients, only the paper and a pen shall be provided with the physical presence of the clients. In other words, the bank intended to redirect clients' signature to an electronic channel regardless of the clients' digital literacy in order to reduce number of paper based documents.

2.2. The Developed Signature Process

As the open procurement procedure resulted, the developer company was Cursor Insight Ltd. who won the competition of German on-line signature verification in 2015 [6]. The kick-off meeting was held in 11-03-2016. The development started in Q2 of 2016 and the pilot phase was deployed in Q1 of 2017. Currently more than one million documents (registration forms, contracts and involved orders) were signed by the clients in the branches of OTP with advanced biometric signatures using this method and the number of involved documents is growing continuously. The developer implemented the next procedure for creating advanced biometric signature in the branches. It can be divided into three parts: registration, signing and verification processes.

- Registration process
    - the identification and authentication of clients has to be performed, as required by law, using public records and official documents,
    - the client has to place several handwritten signatures in a registration form, which contains the natural identification data also.

- Signing process
    - the bank clerk has to identify the clients (as prescribed in the internal policies)
    - the bank clerk prepares the document which has to be signed
    - the bank places a qualified electronic seal and a qualified timestamp, which are issued by a public trust services, on the prepared document
    - the application sends the prepared document to the signing pad for signing
    - the client signs the document with moving a special pen17 on the signing pad
    - the signing pad connects the document and the client's biometric signature using its asymmetric private key which is certified by a public trust service provider
    - the bank places a qualified electronic seal and a qualified timestamp again on the whole document
    - the client gets the signed document through the internet banking system
- Verification process
    - the client requests a verification process on a given document
    - the bank provides a tool or data for performing the verification, including at least the following elements:
        - valid list of signing pads in the bank
        - valid certificates of signing pads
        - the client's registration form including handwritten signatures
    - the validity of qualified seals shall be checked
    - the validity of qualified timestamps shall be verified
    - the validity of non-qualified signature of the signing pad has to be determined
    - matching biometric signature(s) on the document with biometric signatures(s) on the registration form has to be evaluated.

The steps of the signature verification process can be derived from the following figure. All signatures should be verified and validated before the document is accepted. The relations between

[17] It is a battery-free pen using Eletromagnetic Resonance Technology. It means that the sensor is only responding to the pen. Output rate of the coordinates is 500 Hz consisting of x, y, time and pressure.

signatures are sequential from inside to outside. Outermost signature is needed by legal and archiving reasons.

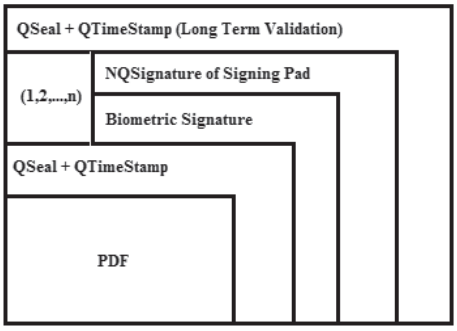

Figure 1: Internal structures of signed documents (Created by the Author)

It is very important that biometric data are used as signature instead of identification. The officer identifies clients by checking the presented identification documents (e.g. national ID card, passport, driving license or banking card with PIN code). This identification process always precedes the creation of biometric signature. Therefore, the bank focuses on verifying biometric signature created by an identified person instead of matching an unknown biometric signature to the one of the recorded biometric data. In January of 2018, IBM published a research material in connection with biometric authentication [8], which is based on a global survey with 3.977 answers, of which 1.976 came from the USA, 1.004 came from the EU and 997 answers came from Australia, India and Singapore. They found that the authentication methods perceived as most secure is the fingerprint usage (44%) and retinal (eye) scan (30%). Oher methods (facial recognition, handprint, voice and heartbeat recognitions) are used cumulatively less (32%) than fingerprint. Using handwritten signature as identification method may occur in less than 2% of responders.

It should be noted that only such signing pads can be used in the bank, which are purchased, installed and configured by the bank, which have a valid X509v3 signing certificate from a public trust service provider listed in European Trust List for theirs on-board generated private keys, and which are not able to accept digital data beyond the signing surface. This condition ensures the validity of signatures. If an attacker tries to forge the signatures and repeat recorded biometric data or any variant of it, apparently real signatures may be created. The verification of these signatures may result in positive answer in a commonly used signature verification tool. In this system, this forgery can be detected, because the validity of the signature requires a valid signature on the document and the client's signature data from a valid signer pad also.

The elements and attributes of a client's signature in this closed system are the following:

- signature creation data: eventually, the signature creation data are the signs of a pencil which is moved by a natural person signatory's hand on the given signing pad. These analogue data are digitized for further processing. The digitized copy of the signature is not applicable for creating a valid signature again, it serves only verification purposes.

- signature validation data: digitized and stored instances of the natural person signatory's

handwritten signatures, which are recorded during the registration process, and the X509v3 certificate of the given signing pad where the signing process is performed.

- it is uniquely linked to the signatory, it ensures by the recorded biometric data and the performed identification process of the physically present client.
- it is capable of identifying the signatory, because digitized handwritten signature can identify the signer physically,
- it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control, hence the signature creation data – attributes of the pencil movements – cannot be digitalized, used or reproduced and injected to the signing pad without the signatory with a high level of confidence, and
- it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable, it guarantees a qualified seal on the unsigned document and a qualified seal with qualified timestamp on the entire document in order to enhance trust.

Steps	Device
Creating document	Front-office banking system (PDF printer)
Preparing document for signing	Signature Device Controller on officer's desktop
Sealing and timestamping document	Crypto-server as back-office banking system
Signing document by client	Signing pad (sensor pad)
Signing document and client's biometric data by signing pad	Signing pad (crypto-module)
Sealing and timestamping document before archiving	Crypto-server as back-office banking system

Table 2: Overview of biometric signing process (Created by the Author)

The data transferred between the signing pad and the officers' computer is protected by encryption. The signature and its biometric properties are resistant to any kind of surveillance or interference. The signature is placed in the document and protected against tampering. The encryption algorithms are accepted by the German Federal Network Agency also. Within the PDF, the signature cannot be manipulated or misused in any way. This has been independently confirmed by an Information Technology expert from TÜV Saarland (Technological Inspection Association) at the request of the manufacturer (general evidence). The whole process was audited by an internal IT and security professional, an eIDAS auditor, a judicial IT expert and it was certified by an accredited certification body in accordance to proving the fulfillment of eIDAS requirements for advanced electronic signatures (special evidences). The above facts prove with a high level of confidence that biometric signatures generated by the above method fulfil the requirements of advanced electronic signature.

3. Discussion and Conclusions

We have attempted to discuss biometric signatures in three dimensions: the legal, technical and business aspects were discussed theoretically, legally and practically. The biometric solutions have several advantages on business side and e-Administration side also, because these are cheap, efficient and using biometry does not require any tools on the client side, but the usage may be

limited because cross-border acceptance of such signatures requires the extension of national laws. Branches in other Member States can use this technology if the national legislation allows creating advanced electronic signature in closed systems. The court practices in this field have been unknown yet, therefore certain legal risks may occur in case of a litigation. It can be reduced by a professional opinion from an electronic signature expert, a legal opinion from a judicial IT expert and a certificate from an accredited certification body, which prove that the given solution fulfils all requirements of the advanced electronic signature. There is still a lack of standards and of the description of evaluation processes for advanced biometric electronic signatures. Numerous standards are available regarding the recording, transporting and storing of different biometric data such as written signature, fingerprint and voice for using these data in authentication procedures. Processing technology of biometric data is developed and used widely as digital data. Hungarian Association for Electronic Signature has issued a professional opinion of applying and using biometric signatures, which declares that most of biometric signatures do not fulfil the requirements of advanced electronic signatures, therefore using such signatures in secure manner require additional measures [4]. Researchers developed mixed methods, which combined public key cryptography (PKI) with biometric data and they claimed that the combination of PKI and biometrics can offer a more secure mechanism, because private keys can be generated directly from the biometric scan [3], [11]. After a decade, this topic appears again [7]. Elliptic curves may also be combined with biometric data as digital signature [9]. The general problem of these ideas is the prevention of successful reusing of recorded biometric data. Other researchers proved that a biometric signature (more precisely the recorded digital data) can be modified and altered in such a way (e.g. combining data with Gaussian noise) that the verification procedure accepts the modified biometric signature as the original handwritten signature. The probability of a successful modification seems to be very low [12].

There is no doubt that the biometric electronic signature can be used as normal electronic signature nationwide until creation and validation methods of advanced biometric signatures will be standardized and widely accepted in the EU. Without cross-border acceptance advanced biometric signature may be used only at national level. It requires the partial extension of related legislations for Pubic Administration (e.g. redefining the client's signature in Hungarian Public Administration). The presented solution can provide advanced electronic signature with full probative force for citizens without e-signature capabilities in e-Administration. This solution can make the digital gap disappear [14], and it is also independent from digital poverty [1] as well as it can be applied in all areas of e-Participation [13] at national level. Effectivity can be enhanced by integrating e-signature devices (e.g. card readers) and biometric signature devices (e.g. signing pads) in Public Administration until remote signature applications are developed. Home and mobile use of this technology is also conceivable, if it is combined with a remote identification procedure (e.g. video identification), and if the security of the signing environment as well as the integrity of the software on the signature capturing device is ensured. For this, however, further innovation will be necessary in the near future.

4. References

[1] CSÓTÓ, M., Aki (információ)szegény, az a legszegényebb? Az információs szegénység megjelenési formái, (Is the poorest the one who is (information) poor? Forms of information poverty), Információs Társadalom, XVII. évf. (2017) 2. szám, 8-29. old. http://dx.doi.org/10.22503/inftars.XVII.2017.2.1, 2017.

[2] Eds. DEMETER, E., PETÉNYI, S., Jelentés a Jó Állam Véleményfelmérésről (Report on the Good State Survey), Nordex Nonprofit – Dialóg Campus, 2017.

[3] FENG, H., WAH, C. C., Private key generation from on-line handwritten signatures, Information Management & Computer Security, 2002 10(4) pp.159-164.

[4] HUNGARIAN ASSOCIATION FOR ELECTRONIC SIGNATURES, Issue of Applying Biometric Electronic Signatures, Budapest, 2016.

[5] Ed. KAISER, T., Jó Állam Jelentés 2017 (Good State Report 2017), Dialóg Campus, 2017.

[6] MALIK, M. I., AHMED, S., MARCELLI, A., PAL, U., BLUMENSTEIN, M., ALEWIJNS, L., LIWICKI, M., ICDAR2015 competition on signature verification and writer identification for on-and off-line skilled forgeries (SigWIcomp2015), In Document Analysis and Recognition (ICDAR), 2015 13th International Conference on (pp. 1186-1190), IEEE, Nancy, France, 2015.

[7] MANN, D., GUPTA, S., SHARMA, A., AKHTAR, S., Digital Signature Using Biometrics, in: Proceedings of the World Congress on Engineering and Computer Science 2015 Vol I, San Francisco, USA, 2015.

[8] KESSEM, L., Future of Identity Study – Consumer perspectives on authentication: Moving beyond the password. IBM Security, Cambridge, USA. 2018.

[9] MOHAMMADI, S., ABEDI, S., ECC-Based Biometric Signature: A New Approach in Electronic Banking Security, In: International Symposium on Electronic Commerce and Security, 2008.

[10] NIST, Special Publication 800-63-3, Digital Identity Guidelines, USA, 2017.

[11] ORVOS, P., SELÉNYI, E., HORNYÁK, Z., Towards Biometric Digital Signatures, in: Networkshop 2002 Conference, Eger, Hungary, 2002.

[12] PARZIALE, A., DIAZ, M., FERRER, M. A., MARCELLI, A., Do synthetic generated signatures reflect the subject motor programs? A pilot study, Proceedings of 18th IGS Conference, June 2017, Gaeta, Italy, (pp. 119-122.), 2017.

[13] PINTERIČ, U., Limitations of the e-Participation, In Hendrik Hansen, Robert Müller-Török, András Nemeslaki, Johannes Pichler, Alexander Prosser, Dona Scloa (eds.), CEE e|Dem and e|Gov Days 2017, Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment? Proceedings of the Central and Eastern

Eurpoean e|Dem and e|Gov Days 2017 May 4-5 Budapest (pp. 89-96), Austrian Computer Society, Vienna, Austria, 2017.

[14] SORIN DAN, S., Digital Divide in the EU countries from the Danube Region, In Hendrik Hansen, Robert Müller-Török, András Nemeslaki, Johannes Pichler, Alexander Prosser, Dona Scloa (eds.), CEE e|Dem and e|Gov Days 2017, Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment? Proceedings of the Central and Eastern Eurpoean e|Dem and e|Gov Days 2017 May 4-5 Budapest (pp. 79-86), Austrian Computer Society, Vienna, Austria, 2017.

eGovernment V

PUBLIC RESEARCH AND INNOVATION INFRASTRUCTURE OF THE REPUBLIC OF MOLDOVA: CHALLENGES AND OPPORTUNITIES

Igor Cojocaru[1], Alfreda Rosca[1], Andrei Rusu[1,2]and Mihail Guzun[1]

DOI: 10.24989/ocg.v331.35

Abstract

Currently the science and innovation area of the Republic of Moldova is undergoing an extensive process of transformation aiming to increase the effectiveness, to facilitate the inclusion of national science into the ERA. Taking into account that the European integration is a major priority for the Republic of Moldova, the public research and innovation sector should comply with the best European and international practices. In this regard, the Republic of Moldova developed Research Strategy till 2020 that provides enhancing the quality and efficiency of administrative processes for implementation of the best innovative measures aiming at the development of human, institutional and infrastructure capabilities. In actual conditions, it is important to align with the European practices, in special with the policies promoted by the European Strategy Forum on Research Infrastructures (ESFRI), which has a key role in policy-making on research infrastructures in Europe, the European Open Science Cloud (EOSC) – a cloud for research data in Europe, background, policy information, events and publications, ERRIS (Engage in the Romanian Research Infrastructures System) - platform for research infrastructures, research & technological services, etc. Nowadays, for science and innovation area of the Republic of Moldova is necessary to build tools for fostering the continuous dialogue between science, Government, society, stimulating the private sector access to research infrastructure, scientific laboratories and results, creating the appropriate conditions for facilitation the process of actual challenges turning into opportunities.

1. Introduction

Currently the research and innovation area of the Republic of Moldova is undergoing an extensive process of transformation aiming to increase the effectiveness and facilitate the inclusion of national science into the European Research Area (ERA). Taking into account that the European integration is a major priority, the public research and innovation sector should comply with the best European and international practices. In this regard in the Republic of Moldova was developed the Research Strategy till 2020 that provides enhancing the quality and efficiency of administrative processes trough implementation of the best innovative measures aiming at the development of human, institutional and infrastructure capabilities. The governmental documents of the Republic of Moldova provide roadmap of science and innovation sector elaboration, one of the main goals of which is the national research infrastructure upgrading by 2020, the connection of national science infrastructure to the European networks, including the efficient use of e-infrastructures and information resources, implementation of efficient technologies and setting-up a favorable environment to dissemination, absorption and exploitation of scientific information in society.

[1] Information Society Development Institute, str. Academiei 5A, Chisinau, Republic of Moldova, {igor.cojocaru,alfreda.rosca,andrei.rusu,mihail.guzun}@idsi.md, https://www.idsi.md/

[2] Ovidius Univercity of Constanta, bd. Mamaia 124, Constanta, Romania, agrusu@univ-ovidius.ro, http://math.univ-ovidius.ro/

The *purpose of the article* is to elucidate the situation in the research and innovation infrastructure of the Republic of Moldova, to underline the needs of this sector developing through innovative informational tools implementation, to select the most acceptable practices for science infrastructure safeguarding and aligning to the best European experiences.

Nowadays for research and innovation area of the Republic of Moldova is necessary to build tools for fostering the continuous dialogue between science, Government, society, private sector, for access facilitating to research infrastructure, scientific laboratories and results. In this connection, a good advice for the Republic of Moldova can be the next phrase „The state must be in possession of the organizational and operational capabilities needed to react to the quickly changing challenges of our times while effectively pursuing the national interest in the face of conflicting regional and global agendas" [16]. Many provocations are arising for Moldovan research area, that's why the Government, responsible entities, everybody should rapidly adapt to the evolving regional and global challenges and contribute to their turning into opportunities.

2. Defining the term "infrastructure", including "e-infrastructure"

Considering that these notions in specialized sources are differently explained, there is no a unique understanding of *infrastructure* and *e-infrastructure*, these terms are viewed and analyzed from different points of view appeared the need of their clarification for the purpose of better understanding of the subject.

The Science and Innovation Code of the Republic of Moldova, approved in 2004, qualifies the *infrastructure of research* as the organizations that carry out scientific and innovation activities: Academy of Sciences, other institutions performing science and innovation, financial ones, business incubators, innovation parks (scientific, techno-scientific and technological), enterprises and other specialized organizations [19, art. 25]. The Oxford Dictionary describes *infrastructure* as basic physical and organizational structures and facilities (e.g. buildings, roads, power supplies) needed for the operation of a society or enterprise [18]. In the American Heritage Dictionary *infrastructure* is an underlying base or foundation especially for an organization or system; the basic facilities, services, and installations needed for the community or society functioning, such as transportation and communications systems, water and power lines, and public institutions including schools, post offices, etc [14]. In Cambridge Advanced Learner's Dictionary *infrastructure* is described as basic systems and services, such as transport and power supplies, that a country or organization uses in order to work effectively [2]. The International Standard ISO 9000: 2015 "Quality Management Systems — Fundamentals and Vocabulary" defines *infrastructure* as a system of facilities, equipment and services needed for the operation of an organization [22].

As an umbrella for all infrastructures in the field of scientific research, *e-infrastructure* is the basic element that helps bring together researchers from different corners of the globe, allows access to scientific data and tools in high-performance laboratories around the world, enables international collaborative research, provides unique services to users from different countries, as well as opens opportunities for young people attracting into science. *E-infrastructure* is an environment where resources (hardware, software and content) can be easily accessed. It provides the scientific community with a 24-hour digital resource market, regardless of location, and serves as a unique tool for collaborative applications developing [5]. Viewed by the UK Research Council *e-infrastructure* refers to a combination and interconnection of digital technologies (hardware and software), resources (data, services, and digital libraries), communications (protocols, access rights

and networks), researchers and organizational structures needed to support modern research, based on international collaboration [7].

E-infrastructure plays an increasingly active role in knowledge advancement, contributes to the creation of innovative environment. It is at the heart of knowledge triangle: research, education and innovation. The widespread use of e-infrastructure is an important step towards digital differences and brain drain reducing.

3. Research infrastructure in the Republic of Moldova

Throughout the history of science, the number of research organizations in the Republic of Moldova varied numerically in different times. Thus, nine research institutes were active in 1960, in 1970 - 66, 1985 - 107, 2004 - 101. In 2017, there were nine research institutes of the Academy of Sciences of Moldova, 33 scientific organizations from different branches, 12 accredited universities, 2 museums, 3 science and technology parks and 7 innovation incubators [11].

At the end of 2014 in the Republic of Moldova was approved the Research and Development Strategy until 2020. One of the basic objectives of the strategy is human, institutional and infrastructure capacities development [13, p. 28]. According to its provisions, this major task is to be accomplished through innovative tools implementation for private sector access facilitating to research infrastructure, scientific laboratories, fostering continuous dialogue between science and society, knowledge disseminating and research results capitalizing [13, p. 51].

For these purposes and in the line with European and international performance standards in the Republic of Moldova in 2010 the knowledge network ACADEMICA was designed and developed [4]. Its main objective is to provide a computerized infrastructure for accessing and sharing scientific and technological information to research institutions and universities, to increase the capacities at a new technological level in order to meet the challenges of implementing the European practices, in special the concept of Open Science. Exploiting the opportunities offered by ACADEMICA e-infrastructure, including interconnection with researchers from other countries, help to strengthen national teams in interdisciplinary project proposals development and joint participation in HORIZON 2020 Program calls. Based on Principles for Open Scholarly Infrastructures and in line with the Amsterdam Open Call for Open Science Action (April 2016), ACADEMICA e-infrastructure will be expanded in the nearest future.

An important public institution in the Republic of Moldova is the Research and Educational Networking Association of Moldova (RENAM), which represent an interoperable collaboration platform that contributes to the convergence of universities and research institutions electronic infrastructure. The principal purpose of its activities is a constant development of communication and information infrastructure of scientific and educational Moldovan communities. [1].

Thanks to the EU projects, several universities of the Republic of Moldova have created their institutional repositories. The software solutions are open-source, namely, DSpace [12]. In addition to the institutional repositories, there is a national repository, created by the Information Society Development Institute, named National Bibliometric Instrument (IBN) [15], where scientific publications are stored. Public scientific libraries in the Republic of Moldova are equipped with computers connected to the Internet, some of them provide access to other electronic resources through collaborative agreements with international organizations (Research4Life) [20].

In the period 2009-2012 Moldovan researchers together with 19 partners from 10 countries implemented the SEERA-EI (South East Europe Space for e-Infrastructure Research Area) project [21]. The main objective was to develop and strengthen the coordination and cooperation of e-infrastructure programs in the South East Europe region. This project has paved the way for sustainable regional co-operation. Within the project was developed the "Common Regional Vision and e-Infrastructure Strategy", which sets out a mutual strategy for e-infrastructure development in the South East Europe region. The elaborated Memorandum provides for a fiber backbone network to be set up in the South East Europe region by 2020. The SEERA-EI and other related regional projects focused on e-infrastructure development issues have enabled the foundation of modern electronic infrastructure and related services in the Republic of Moldova. The permanent upgrading of e-infrastructure components is in the line with the Europe's overall objective - accelerating the development of the information society in Europe, ensuring its availability for all the communities.

In this regard, the Information Society Development Institute of the Republic of Moldova is working on innovative tools creation for research system monitoring and evaluating, indicators of scientific production measuring, system mapping via innovative methodologies for information studying and processing. The Information Society Development Institute performs activities oriented:

- on shareable e-infrastructure development for a better use of the services provided by local administration, European e-infrastructures;

- on Open Science principles implementation through software tools development, such as National Bibliometric Instrument (ibn.idsi.md), Expert Online (expert.idsi.md),

- on acquisition and setting-up of equipment for digital identity (IdP, SP) management, mobile access (EduRoam),

- on consequently provision of secure, reliable access to systems and services available in ACADEMICA and other European e-infrastructures,

- on establishing, together with RENAM (the national NREN), a national federation of research identity providers.

4. European research infrastructure policy

The European Union undertook several initiatives to support the advancement of research infrastructures and e-infrastructure, in particular as an important tool for the development of scientific research in general. The European Strategic Research Infrastructure Forum (ESFRI) [10] determines the overall policy on research infrastructure in Europe. ESFRI's mission is to facilitate multilateral initiatives for better use and development of research infrastructures at EU and international level. ESFRI develops recommendations for ensuring equal access to European resources. Open access to advanced digital services, scientific tools, data, knowledge and expertise that researchers need to collaborate and achieve excellence in science and innovation is a central goal of European policy. The EU believes that the whole community must be engaged in the governance, management and conservation of these resources for the people benefit.

In order to solve some strategic issues regarding the development of e-infrastructure components, the European Commission established in 2003 a special e-Infrastructure Reflection Group (e-IRG)

[9]. The e-IRG vision is an *open* and *innovative* e-infrastructure that offers flexible cooperation and optimal use of available electronic resources by international communities. E-IRG coordinates pan-European initiatives and joint electronic infrastructure development projects for research and innovation in Europe. The European Union recognizes the decisive role of e-infrastructure in achieving scientific excellence, its major contribution in attaining the objectives of Digital Agenda for Europe and vision for the European Research Area. Electronic infrastructures enhance research creativity and efficiency; reduce the gap between developed and less developed countries.

In this regard, was analyzed the innovative informational platform ERRIS (Engage in the Romanian Research Infrastructure System), a register of research infrastructure in Romania [24]. ERRIS was launched in mid-2015 in order to increase visibility and facilitate access to Romanian research infrastructure. This platform has been developed to support and promote Romanian public / private research infrastructure, to stimulate collaboration and participation in national and international networks. The platform makes research more open and transparent, contributes to the effective use of available scientific equipment, increase the visibility and facilitate access to it. The ERRIS platform is considered a "facebook of things" of Romanian research community. Currently, ERRIS brings together 1.611 infrastructures with 8.331 research services, 140 technological services and 22.203 equipments (situation 10.03.2018). So, this example from an EU member country is necessary to follow in the Republic of Moldova and today the Information Society Development Institute is taking steps for the creation a similar “facebook” of the Moldovan research infrastructure.

5. Research infrastructure components

The Manual ISO 9001:2015 Quality Management System stipulates that organization is responsible for planning, providing and maintaining the resources needed to achieve product and process conformance, including buildings, workspace and associated utilities, process equipment (hardware and software) and supporting services [23, see 7.1.5]. Thus, the infrastructure includes:

- buildings and associated utilities,
- equipment, involving hardware and software,
- transport resources,
- information and communication technologies.

According to the Frascati Manual (edition 2015) [17, p. 31] for the area of science and innovation, the basic components of infrastructure are:

- lands and buildings,
- machinery and equipment,
- capitalized computer software,
- other intellectual property products.

6. Research infrastructure maintaining and developing in the Republic of Moldova

In order to align with the principles of Open Science [6], the most important goal of the next European Program Framework, the Information Society Development Institute coordinates its activities with local governmental organizations, with different international institutions, tries to implement the best practices. The institute is going to create an online platform of infrastructure in the field of science and innovation. The beneficiaries will be the scientific community (researchers, professors, PhD students, students), those responsible for managing RDI activities, experts, institutions involved in creation, archiving and dissemination of digital scientific content, organizations responsible for policy implementation, business sector. The society will benefit from open access to scientific heritage of the country; the results will be used in bibliometric and webometric analysis. As a result of data collection, administration, processing and interpretation services, it will be possible to generate: specific lists, reports, organizational charts, diagrams and graphs, statistical and comparative data. More quality data available to policy makers in the Republic of Moldova may lead to a better management of its research.

For Moldovan researchers' cohesive actions and e-infrastructure developing are important, the services provided by:

- LEAF - Identity Federation for Research and Education Institutions of the Republic of Moldova,
- EDUROAM - unlimited Wi-Fi access to scientific and educational community around the world,
- eduGAIN - unlocking global collaboration in education and research, Federation as a Service - federative link to resources and data,
- GEANT Cloud Services - services that support cloud-based collaboration,
- GEANT Open - Facilitating Open Collaboration Globally,
- GEANT VPN Services - service for private and secure connections designed to create global cross-border research teams,
- perfSONAR - real-time monitoring of multiple performance ranges,
- Performance Enhancement Response Team - support service within the community to achieve maximum network performance,
- eduCONF - improving access to video conferences,
- eduOER - support for accessing media content from various repositories,
- RENum.net - interconnecting different ways to dial for real-time connections.

These technologies mainly deal with e-infrastructure, so, as a conclusion, a better e-infrastructure management based on innovative e-services and e-tools is a must do.

The research infrastructure platform, which will be elaborated, will facilitate integration of scientific community into the European information system of databases, serving as a support in management activities. The mapping of existing organizations, equipment, products and research services in the Republic of Moldova will contribute to:

- visibility and transparency increasing;
- science governance facilitating;
- quality and efficiency of science management enhancing;
- use and share of scientific equipment rising;
- cooperation at national and international level stimulating;
- new partnerships between research entities and private sector establishing;
- research institutions competitiveness increasing;
- expertise process facilitating;
- an overview of national research ecosystem providing;
- an engine of internationalization and promotion of research serving;
- governance and management science system strengthening;
- role of science in society increasing.

7. E-Government for research area

The achievements in the information technologies have changed the communication process between citizens, science and Government. The efforts made by the Moldovan Government to accelerate the development of complex e-services with reference to research e-infrastructure have the goal to ensure effectiveness of e-services and reduce the administrative burden. In order to enhance the quality and efficiency of administrative processes and public services in the Republic of Moldova was created the institution "E-Government Center". The aim of this organization is to improve the governance quality through a wide application of information and communication technologies in all areas. For security assuring in the field of e-infrastructure and for important strategic relationships building was developed the Cyber Security Center CERT-GOV-MD. Its mission is to increase the capability of M-Cloud beneficiaries, public administration authorities, Moldova's critical information service providers, to respond to vulnerabilities, threats, and information security incidents in order to protect ICT infrastructure and preserve trust in governmental information system [3].

An important role plays the Platform of Electronic Services that offer citizens the possibility to authenticate to government and public authorities' e-services, similar to national federation of identity providers LEAF, with the aim to unify the scheme of access to any e-services [8]. Another e-service, offered via e-government is the MPay, which allows paying in a secured manner.

8. Conclusions

The officials of the Republic of Moldova have to recognize that a strategic role in increasing the country's competitiveness, in ascending economic prosperity, lies in the area of science, technological development, and innovations implementation. To achieve the goal of better competitiveness the civil society of the Republic of Moldova and its elected representatives should follow the best practice of EU countries. In order to maintain and develop the infrastructure in the Republic of Moldova, essential support from the state is required, more active involvement in realization of as many international projects as possible, supporting the performance, endowing science with modern equipment, taking over the best technologies. In the area of informational support for science and innovation, the best things that can be done are the next concrete examples:

- to continue efforts to get a platform of the available research infrastructure,
- to establish a functional and widely used federation of identity providers and service providers,
- based on the federation of identity providers to support creation of virtual research teams, which involve researchers from the Republic of Moldova,
- to wider the use of services based on GEANT network,
- to facilitate the concept of open science, including the concept of open data in Government's policy regarding research.

The maintenance and improvement of research infrastructure with permanent Government support and efficient coordination must become a primary task in the country's policy. This desideratum needs to be developed around strategic areas, necessary for state, and synergistically correlated, so as to strengthen the infrastructure, maintain and advance the tendency of integration in the European Union. Under the current circumstances, through information innovative tools it is important to create a simulative and favorable environment for private investment in science, for dialogue and cooperation encouraging between politics, administration, civil society and citizen, and promoting efficient public-private partnerships.

Acknowledgments. Special thanks to the SCIFORM national project (15.817.06.13A) and E-IDSM research project (18.50.07.10A/PS) that have partially supported research on this paper.

9. References

[1] BOGATENCOV, P., SECRIERU G., TIGHINEANU I., E-Infrastructura RENAM – platforma interoperabilă de colaborare, resurse şi servicii informaţionale în cercetare şi educaţie, Akademos, nr. 2 (45), 2017, https://ibn.idsi.md/ro/vizualizare_articol/53338

[2] CAMBRIDGE UNIVERSITY PRESS, Cambridge online dictionary, Cambridge Dictionary: English Dictionary, http://dictionary.cambridge.org/dictionary/english/infrastructure?a=british (accessed 26.10.17)

[3] CERT-GOV-MD, Cyber security center, http://cert.gov.md/ (accessed 15.10.17)

[4] COJOCARU, I., Knowledge Networking – a Promising Tool for Developing Moldova's R&D, in: Proceedings of the International Conference on Intelligent Information Systems IIS-2013, August 20-23, 2013, Chisinau, Republic of Moldova, https://idsi.md/files/file/publicatii/2013/Knowledge%20networking_a%20promising%20tool%20for%20developing%20Moldovas%20RD%20protential.pdf

[5] CORDIS, Community Research and Development Information Service, http://cordis.europa.eu/ictresults/home_en.html (accessed 18.10.17)

[6] CREATIVE COMMONS, Science Commons, http://sciencecommons.org/resources/readingroom/principles-for-open-science/ (accessed 20.11.17)

[7] DEPARTMENT for Business Innovation and Skills, Delivering the UK's e-Infrastructure for Research and Innovation, Technical Report, UK Research Councils, 2010, http://www.rcuk.ac.uk/documents/research/esci/e-infrastructurereviewreport-pdf/

[8] EGC, Portalul serviciilor electronice, http://e-services.md/ (accessed 10.12.17)

[9] E-IRG, E-Infrastructure Reflection Group, http://e-irg.eu/ (accessed 22.11.17)

[10] EUROPEAN COMMISION, European Research Infrastructures, http://ec.europa.eu/research/infrastructures/index_en.cfm?pg=esfri (accessed 28.11.17)

[11] DUCA, Gh., Ştiinţa şi inovarea în Republica Moldova: istorie şi actualitate, Akademos, 1, 2017, 92-103, http://www.akademos.asm.md/files/92_104_Stiinta%20si%20inovarea%20%D0%Ben%20Republica%20Moldova_istorie%20si%20actualitate.pdf

[12] DURASPACE, http://www.dspace.org/ (accessed 15.12.17)

[13] GOVERMENT of the Republic of Moldova, Strategia de cercetare-dezvoltare a Republicii Moldova până în 2020, Goverment of the Republic of Moldova, Chisinau, 2013, http://www.asm.md/galerie/2013_11_25_Str_CD-2020_FINAL.pdf

[14] Houghton Mifflin Harcourt, The American Heritage Dictionary of English Language, Houghton Mifflin Publisher, 2015, https://www.ahdictionary.com/word/search.html?q=infrastructure (accessed 12.10.17)

[15] IDSI, Instrumentul bibliometric national, http://ibn.idsi.md/ (accessed 12.11.17)

[16] KASER, T. (ed)., Good State and Governance Report 2015, National University of Public Service, 2015, Budapest, Hungary, http://archiv.en.uni-nke.hu/uploads/media_items/good-state-and-governance-report-2015.original.pdf

[17] OECD, Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264239012-en

[18] OED, English Oxford Living Dictionaries, Oxford University Press, UK, https://en.oxforddictionaries.com/definition/us/infrastructure (accessed 14.10.17)

[19] PARLIAMENT of the Republic of Moldova, Cod nr. 259 cu privire la știință și inovare al Republicii Moldova, Monitorul Oficial, nr. 125-129, 30.07.2004, http://lex.justice.md/index.php?action=view&view=doc&id=286236

[20] RESEARCH4LIFE, http://www.research4life.org/ (accessed 05.12.17)

[21] SEERA-EI Project, Deliverable D4.1a. SEERA-EI-Interim Report-b-2011-7-22, 63 p.

[22] Technical Committee ISO/TC 176, ISO 9000:2015 Quality management systems — Fundamentals and vocabulary, Standard, International Organization for Standardization, Geneva, CH, https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en

[23] Technical Committee ISO/TC 176, ISO 9001:2015 - Quality management systems – Requirements, Standard, International Organization for Standardization, Geneva, CH, https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:en

[24] UEFISCDI, Engage in the Romanian Research Infrastructure System, http://www.erris.gov.ro/index.php (accessed 15.12.17)

INTEROPERABILITY: HOW TO IMPROVE THE MANAGEMENT OF PUBLIC FINANCIAL RESOURCES

György Nyikos, Bálint Szablics and Tamás Laposa[1]

DOI: 10.24989/ocg.v331.36

Abstract
The article deals with the application of interoperable digital solutions in the domain of public financial management in order to improve the effectiveness of administrative procedures.

The practical relevance of the topic is derived from the Digital Single Market Strategy for Europe which promotes the interconnection of public portals to elevate the added value of the digitisation of public services. The interconnection of portals and electronic registers can notably facilitate the reduction of administrative burdens, foment the creation of new digital services and contribute to the creation of the Digital State. Nonetheless, there has been little research on how it works in practice and on its impact on the efficiency of public financial management.

The paper systematically reviews the main concepts of public financial management and the relevant strategies on the interoperability of public services. Based on this, it aims to analyse a series of Hungarian practices on interoperability to identify success factors that could support the design of new digital solutions to improve the management of public financial resources.

Keywords*: interoperability, public financial management, e-government, public data*

1. Introduction

Public financial management (PFM) determines the way governments treat public revenues and expenditures and their medium-to-long-term impacts. These procedures and the functions of public financial management are backed by various information systems and their utilization has shown an exponentially growing tendency in the past two decades. There is an abundant literature on the evaluation and comparison of these systems, which are frequently categorized according to main functions, types of service provider or as to the modernity of the applied technology.

The new digital technologies are transforming our society and economy and are opening up new opportunities in the field of PFM as well to improve public services and make a better use of the available public data. In this transformation process, the connectivity of information systems and their capabilities to exchange data (*interoperability)* plays a crucial role.

This paper has three main aims. First, to review the institutional, legal and technological background of PFM in Hungary; second, to highlight the most relevant issues of interoperability; third, to analyse national PFM information systems from the perspective of interoperability and draw conclusions for their future development.

[1] All National University of Public Service, Budapest

2. Public finance management in Hungary

Public Financial Management relates to the way governments manage public resources (both revenue and expenditure) and the immediate and medium-to-long-term impact of such resources. PFM systems are embedded in broader sets of processes, systems and institutions as depicted by *Figure 1*.

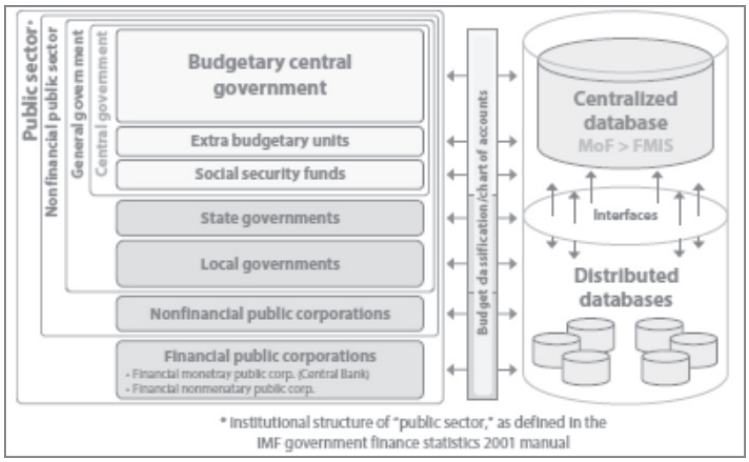

Figure 1: Origin and scope of public financial data [3]

PFM systems are deeply studied and monitored by the World Bank Group (WBG) mainly with respect to its aids and operations in developing countries. WBG and other international organizations finance several projects aiming at the development of PFM systems to increase the efficiency and effectiveness of the use of public sources. Not only the financed countries are in focus, but WBG also keeps track of other nations' activities on this field [23]. Moreover professionals have worked out an evaluation scheme in order to make these systems comparable and published their experiences in PFM development [16].

Analysis of different systems led to a grouping of functions [13]. The eight functional groups represent various fields of public administration not equally supported by integrated IT solutions. It is clear that state revenues and liquidity are two key elements of financing public expenditures, thus it is not surprising that Treasury System Account Management Systems (TSA) and Tax/Customs Management Information Systems (Cust MIS; Tax MIS) were the first to spread. From the late 2000's the penetration of Financial Management Information Systems (FMIS) gradually took the lead[2]. The spread and evolution of PFM systems is shown by *Figure 2-3*.

[2] Consider the fact that by this time internet penetration reached 40 % in developed countries according to ITU.

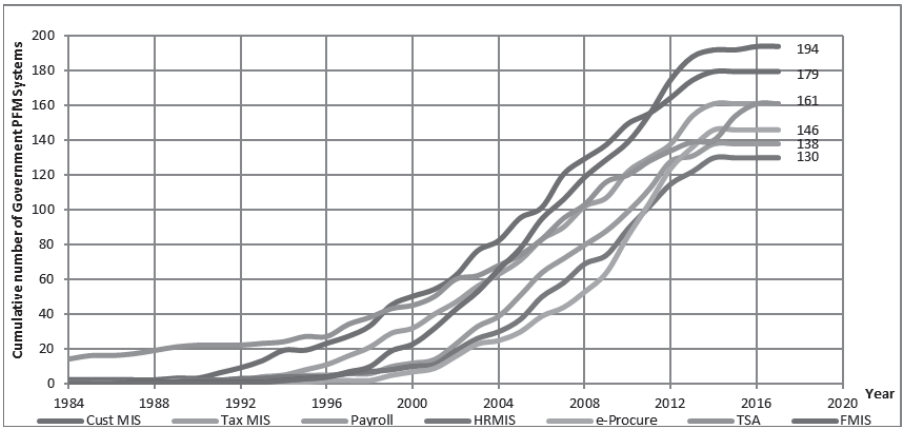

Figure 2: Services of PFM systems [22]

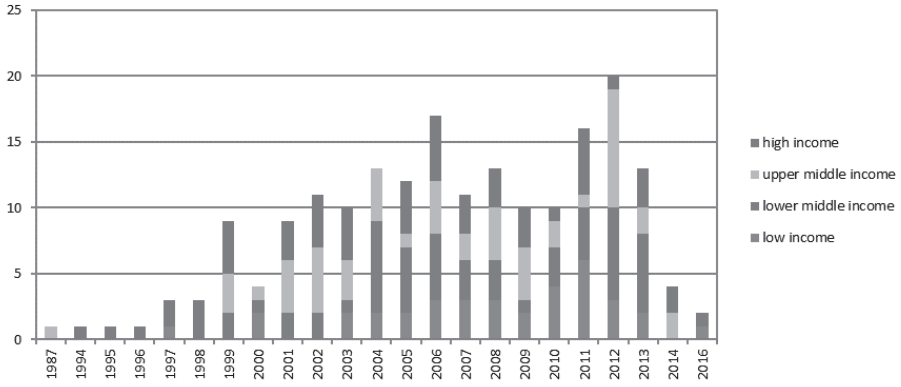

Figure 3: Year of implementation of FMIS solution in use vs. category of GNI per capita [22]

In another study researchers reveal [4] that usage of off-the-shelf systems is proportionally similar to the application of usually older and locally developed ones even if new solutions give a complex answer to governments' needs.

Among the various functions of FMISs, the topmost purpose is to cover all relevant procedures and the provision of a timely database to give a crutch to fiscal and other policy- and decision-makers. Budgetary cycle starts with budget preparation that constitutes the aggregate numbers of a law (or other legislative act) on state budget. The breakdown is made by the Spending Units (SPU), which is applicable for the execution of the budget and the calculation of cash-flows and the definition of other financial needs of the government.

Budgetary management requires a complex information system in view of the following factors: the large number of SPUs; the frequent modifications made within the budgetary year; market impacts on nominal revenue; the overlap of cycles of different budgetary years. Thanks to modern IT solutions and the spread of new technologies, it is becoming easier to tackle all these factors at the same time. A robust and integrated software provides the most suitable solution to meet all these

needs. Nevertheless the WBG and other similar projects' experience show that such developments can take 6-7 years [4].

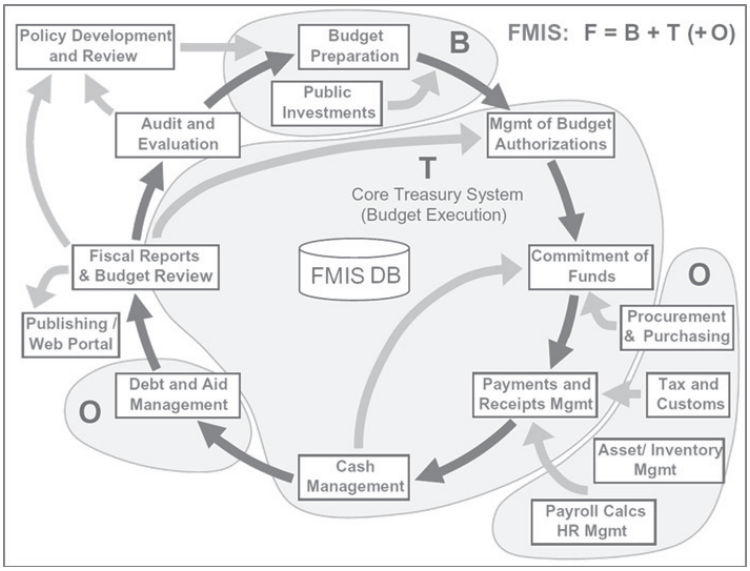

Figure 4: A modular approach for building FMIS [4]

According to the above research, there are modular systems (*Figure 4*) which originate from the business sector and are adapted to public finance specialities (e.g. Oracle, SAP). Although these solutions have an extended world-wide advisory network and they are perfectly fit for a business environment, they mainly focus on manufacturing and not the specificities of public financial management. In the latter decades a few new-wave answers emerged on the market (e.g. Freebalance, Unit4) focusing on the financial sector and or merely on public financial management. Although these off-the-shelf software can be tempting as they promise to be ready for use with a little bit of fine tuning, this can also be a pitfall as the accurate planning cannot be carried out without a good understanding of current and future procedures. This situation recalls the legendary reply of Euclid to King Ptolemy: '*there is no Royal Road*'. As a consequence, research shows that governments are reluctant to change the current systems used for PFM even though new technologies may offer great progress in terms of efficiency.

3. Relevant issues of interoperability

New digital technologies[3] are transforming our society and economy and are opening up new opportunities for public administrations as well. With these technologies it is possible to gather, manage, distribute and analyse data in order to improve efficiency and develop new services. In line with the recent technical developments, countries are *digitising their public administrations* to save time, reduce costs, increase transparency, and improve both data quality and the delivery of public services. There is still a great potential to further improve public services through end-to-end integration and automation, making better use of reliable sources of information and openly

[3] cloud computing, big data, artificial intelligence and the Internet of Things (IoT)

publishing public data while ensuring that citizens' and businesses' records are treated in accordance with data protection rules to increase trust and confidence. Data is at the heart of all new technologies. However, *data management* is not entirely a technical issue; data access, transfer and liability are more difficult and less mature topics that deserve further assessment.
To achieve the possible results using the new digital technologies there are several EU policy initiatives in place, such as:

- the *Digitising European Industry (DEI)* policy package that included the *European Cloud initiative* [6] aiming to deploy a high capacity cloud solution for storing, sharing and re-using scientific data;

- the revision of *the European Interoperability Framework* [7], which aims to improve digital collaboration between public administrations in Europe and will benefit directly from the free flow of data;

- the EU's *commitment to an open Internet* [5]

The so called *PSI directive* [10] was created to provide a legal framework for the commercial utilisation of public sector information. The re-use of public sector data has been proven to increase economic growth and creates a large number of jobs in the SME sector. The directive harmonised the different rules and practices in member states and sought to avert the barriers represented by charges and different data formats to bringing out the full economic potential of public sector data.

On the other hand the relatively new *General Data Protection Regulation (GDPR)* provides a single set of rules for the entire EU, ensuring a high level of protection of personal data. Public sector entities processing personal data must comply with these rules as well. It is important to notice that GDPR prohibits restrictions on the free movement of personal data within the Union where these are based on reasons connected with the protection of personal data [13].

In this transformation process *interoperability* is an essential prerequisite for a competitive well-functioning digital system. It allows administrative entities to electronically exchange information in ways that are understood by all sides. It contains different aspects that impact on the delivery of digital public services, including:

- *organizational interoperability* ensuring the formalization of the processes (modelling) and the interoperability of the models and the harmonisation of administrative systems (i.e. it has several normative elements). Interoperability at organizational level prefers multilateral solutions for everyone instead of bilateral solutions;

- *functional interoperability* meaning the ability of systems to exchange data with each other where the provider issues data that can be interpreted;

- *semantic interoperability* ensuring the use of common descriptions of exchanged data;

- *technical interoperability* ensuring the introduction of necessary information systems environment to allow an uninterrupted flow of bits and bytes (technologies, standards, policies);

- *legal interoperability* ensuring that legislation does not impose unjustified barriers to the reuse of data in different policy areas, guarantees the regulatory background where the cooperating organizations have the appropriate legal power to implement the data exchange in line with common standards. Since public administration can only perform an interoperability act after ex-ante legislation is in place, ensuring this component is an elementary condition;

- *political interoperability* provides the central power and support to achieve implementation and management of public administration interoperability. Here, we can differentiate both national and international dimensions.

The *Interoperability Solutions for European Public Administrations (ISA) programme (2010-2015)* [11] and its successor *the ISA programme (2016-2020)* [12] are the main instruments through which the current European interoperability strategy and European interoperability framework have been implemented. This has involved a variety of actions that aimed to improve digital collaboration between public administrations in Europe. The national interoperability framework observatory (NIFO) [8] measures progress and monitors the state-of-play of interoperability in the Union.

The Hungarian White Paper [1] is one of the outcomes of a 2015 Government Resolution [15], to set the groundwork for open data policies and activities. The document makes seven recommendations:

- Set higher open data targets than required by the EU;

- Actively encourage the use of open data, to create market opportunities and generate growth;

- Create a national data repository that can also host private sector open data;

- Make data available for free or at marginal cost;

- Create an organisation that specialises in the open data process;

- Consolidate the provision of data; and

- Start as soon as possible.

The documents also suggest that the government of Hungary should redouble its efforts to make public sector information available as open data, and actively help to create market opportunities. Recently Hungary began an overhaul of its Government Portal for Digital Services (Magyarorszag.hu), it is upgrading existing services and adding new ones [18]. The new portal aims to increase IT security and to make it easier for companies and citizens to access public services electronically.

4. Public finance information systems in Hungary

If we look for PFM IT solutions in Hungary from the perspective of interoperability, a series of information systems and online services can be found. These systems are operated by the State Treasury and other ministries providing digital solutions and online services in order to make public finance management more effective.

4.1. Public financial management (PFM) systems

The PFM modernization process in Hungary started with a WBG operation in 1996. The project documentation shows that the main goal of the USD 7.7 million project was to reform the PFM system laying down the basis of TSA and establishing the Hungarian State Treasury (HST). The concept comprised a proposition on information centralisation to handle all public financial accounting transactions of the budget [20, 21]. The envisioned concept is depicted by *Figure 5*.

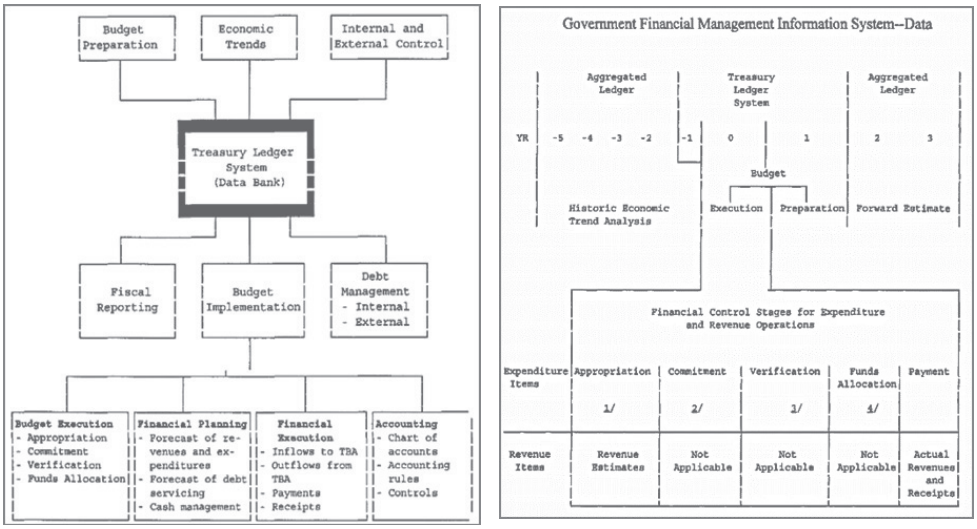

Figure 5: Vision drawn up by project documentation in 1996 for the Hungarian State Treasury [21]

In the middle of the 1990's the Hungarian State Treasury was set up by government resolutions (1128/1994. (XII.30.) and 2189/1995. (VII.4.) in order to realize the goals above and started its operations with a predominantly banking approach. Consecutively the State Audit Office carried out an audit that found that the budgetary planning phase was not adequately prepared compared to the complexity of control procedures, institutional workflows, and security requirements. Thus, – as the mentioned report says – the IT system created differed fundamentally from the immature system design.

In reality the evolution of PFM in Hungary yielded a very fragmented structure in the last two decades. The SPU accounting systems and the core treasury applications have been connected predominantly by the means of human interactions, although the level of ICT would enable to have a much more automatized scheme. Thus it is very expensive to provide human capacity to supervise data correctness as the number of transactions is increasing. Nonetheless supervision produces errors that can also be corrected by human intervention. Last but not least, working out consolidated data – that shows government performance on macroeconomic level – is also challenging with a diffuse system structure. The links among the HST systems are depicted by *Figure 6*.

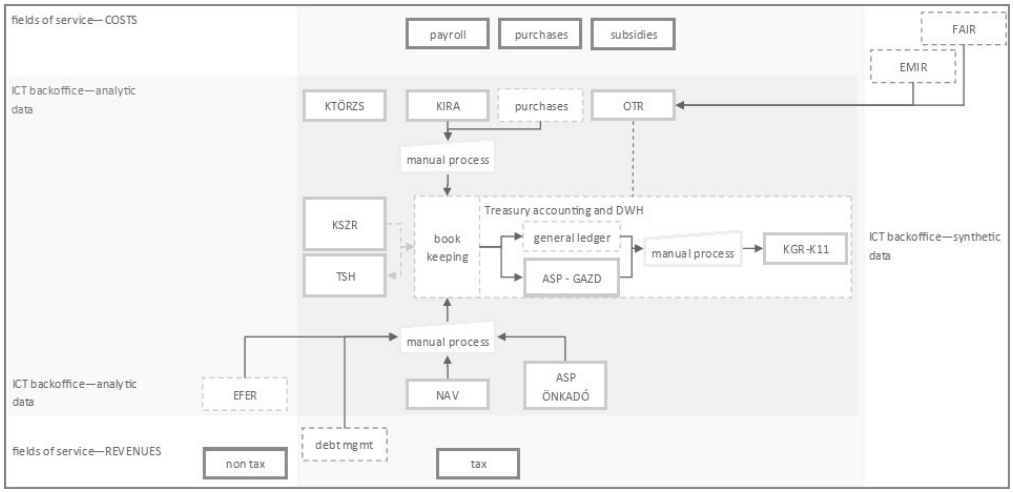

Figure 6: Cooperation of PFM systems

4.1.1. K-Törzs

One of the key elements of the budget execution is the so called K-TÖRZS, which consists of the master data of budgetary bodies not only in the central government but also on a local level. The data are published on the HST website and database is nominated as an authentic register by the law. This means that the data retrieved from in the database represent legal evidence. Besides real time data queries, historical data are also available on the website in order to have a traceable picture on the predecessors. Founding documents of budgetary organisations are published that comprise essential information on the activities, field of operation, leadership and main structure [19].

4.1.2. KIRA

The KIRA system centrally manages the payroll system for all public servants and general government employees. This means that ca. 900.000 people can get their monthly earnings by means of KIRA. The system is the primary information source for the accounting transactions of salaries and provides the basic documents for bookkeeping. Hence it is crucial for all stakeholders to keep the system up-to-date and to do the corrections needed on time.

KIRA strongly cooperates with the K-TÖRZS system mentioned above and produces output information for taxes paid by the single SPUs, payroll for the employees and naturally transfer data packages for the banking system. For some reasons the latter is not forwarded automatically but checked manually by SPUs [19].

4.1.3. KSZR

Payments of central government entities (and some other institutions forced to do so by law) are managed by the core banking system connected to Treasury System Account. Before the middle of the 90's this role was fulfilled directly by the Central Bank of Hungary but – in line with recommendations of the IMF and the WBG – the creation of TSA was a key motivation for the establishment of the Hungarian State Treasury in 1996. In the following years the task of management of public debt was transferred from HST to an agency which marked a clear borderline

between the two institutions responsible for the liquidity management of the central budget. These days the core banking system of the Treasury consists of several subsystems where several interactions are made manually. Some of the budgetary controls are also provided by these systems that prevent the overspending of appropriation limits set by the budgetary law [19].

4.1.4. TSH

The main control element of the appropriation management system is the TSH. This component cannot be directly accessed by SPUs but they can reach it via some other information channels. Certain parts of the procedure are still paper-based, while other procedural elements are automatized via a form filling application. The cooperation of several system elements is strongly manually-backed while the everyday reconciliation with core banking system is automatized. The transactions of appropriations and financial flows are updated regularly and these data are taken (manually) to the reporting system [19].

4.1.5. ASP

For the municipalities the HST is developing a set of cooperating applications called ASP. These cover filing of documents, accounting, local taxation, property management, etc. as a standard service for the SPUs in their scope [19].

4.1.6. KGR-K11

All SPUs in Hungary are forced to hand in regular reports to the Hungarian State Treasury. Budgetary spending (special P/L statement) is reported monthly, balance sheets are provided quarterly and the submission of a yearly accounting report is also required. As the transactional level of accounting is not controlled centrally, the consistency check of these reports are made by the system itself during the submission of reports by means of complex pre-defined controls. According to latest developments, a ledger (backing the numbers of the specific report) is provided by the institutions in a standard format. (Earlier the consistency checks were done manually.) [19].

4.1.7. OTR

The Hungarian State Treasury is responsible to maintain a database on the data of subsidies provided by any budgetary institution. The system has a strong legal background since it is expressed in the law that those grant schemes and agreements are legally non-existent which are not registered in the OTR. According to these legal requirements all fund holders need to send the main decision making and contracting data via a specific interface to the OTR to check the double financing of the operations. Based on these checks, the OTR provides information on the results of checking through the above interface to fund holders. Besides the above functions, the OTR also supports the controls operated by the State Aid Monitoring Office according to rules set by the EU [19].

4.2. Development policy database and information system (FAIR)

Besides domestic development sources Hungary uses substantial amounts of EU funds to finance development projects. Additionally to the earlier mentioned PFM IT modules, the so called FAIR system has been established. The FAIR system serves for the collection of development policy data to create an extensive database on the implementation of different (European, national, other)

development funds. The FAIR provides support for the complete development policy cycle. It is an integrated solution to plan, implement, measure and monitor different development programmes with specific procedures in a unified manner. The unified monitoring and management concept ensures comprehensive decision-making in the field of development policy. The FAIR system is depicted by *Figure 7*.

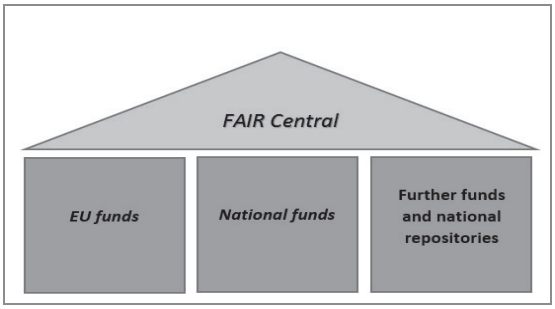

Figure 7: Schematics of the FAIR system

The FAIR realizes a unified monitoring and management concept via the connection of different specialized subsystems and data interfaces. The unified data structure of system components makes the monitoring data of different funds comparable and enables the unified measurement of programmes. The FAIR Central collects financial and physical monitoring data from other subsystems and data interfaces. The FAIR has specialized subsystems providing paperless fund management solutions for national and European funds. These management subsystems provide a specialized e-government portal for beneficiaries and online management modules for institutional users. These management systems are interoperable with the FAIR Central and transfer the relevant data automatically [14].

The scope of pertinent budgetary appropriations is defined by a specific government regulation on the central monitoring of funds. According to this regulation, funding institutions can use the above subsystems or develop their own management systems. In the latter case, the responsible institution needs to ensure that the in-house system collects all relevant data necessary for the unified monitoring concept. These data need to be periodically transferred into the FAIR via a statistical interface according to a pre-defined data format. Thus, external systems need to be interoperable with FAIR in order to ensure the compliance with the unified data structure. It can reasonably be assumed that interoperability plays a crucial role in ensuring data quality and the realization of a comprehensive monitoring concept.

The scope of necessary data is set out in the above regulation as two specialized data groups (one for financial instruments and one for non-refundable grants) taking into consideration the different types of funding. The set data scope covers the following: *project data, data on project owners, data on the implementation and life cycle of projects (appraisal, decision-making, contracting, payments, progress reports, on the spot checks)*. These data (*typically dates, financial and physical indicators and decision data*) encompass the data structure of the unified monitoring concept [14].

As regards interoperability, the FAIR interfaces with several national data repositories (*registry of budgetary organisations, company registry, civil registry*) as well. These data connections enable funding authorities to retrieve valid data on project owners while checking the documents submitted by applicants and beneficiaries. By means of these functions data can be checked against authentic data sources without leaving the monitoring system. Certain data can be retrieved by project owners

while completing administrative tasks in the e-government portal. In this manner certain data fields are auto-filled by the system, so the lead time of administrative tasks can be reduced. Since these data originate from state repositories, they do not necessarily need to be controlled by the funding authorities. In this way interoperability can significantly contribute to the reduction of administrative burdens [14].

5. Future trends and opportunities in public financial data management

The above examples highlight that to support a complex, modern PFM system several functions of the IT system are necessary and interoperability plays a significant role in the development and proper functioning of these PFM systems, and they show how the sharing of public data creates added value. However, there are further unused possibilities to improve the functioning of these systems and the utilization of the available data. It is reasonable to assume that interoperability and data sharing will remain a remarkable factor in the development of these IT systems in the long run. It is thus supposed that the analysis of the main drivers of interoperability may help in formulating assumptions on the future development trends and opportunities of this sector. The table below recapitulates the main information of the systems presented above.

System	Main purpose of the information system	Data scope	Main drivers of interoperability
K-Törzs	Public database of budget entities	Central and local government bodies	Core master data for budgeting
KIRA	Payroll system	All civil servants and employers	coherent data, effective employment
KSZR	Core banking system for SPUs and other public bodies	Payment management and banking services	Liquidity management
TSH	Database of appropriations	Central budget spending surveillance	Efficient budget execution
ASP	Group of applications for municipalities covering key fields of activity	Municipalities' economic activities	Effective common IT background for municipalities
KGR-K11	Reporting on accounting data of SPUs	Accounting data of all SPUs	controlling, reporting to the Parliament
OTR	Monitoring system of subsidies	Donations and subsidies made by government bodies	Efficient allocation
FAIR	development policy decision support, unified monitoring	data on projects and project owners, implementation data	reduction of administrative burdens, data quality

Table 1: Comparison of Hungarian public finance information systems

Comparing the main drivers of interoperability in case of PFM systems it can be assumed that several IT development projects were mainly focussed on the efficiency and effectiveness of budgetary procedures. The creation of a coherent data structure and a strong support for data analytics is another significant driver.

In the case of development policy, the utilization of interoperability and data sharing is twofold. First, they are utilized to reduce the administrative burdens of project owners and funding authorities. Second, the unified collection of relevant monitoring information improves data quality and facilitates more comprehensive policy decisions. The FAIR concept could be treated as a special example that could be realized in other policy sectors as well. Unified databases provide a better view on the progress and implementation of sectoral policy objectives. This requires a sectoral monitoring concept, the definition of shared data, and the development of a common database and the interoperability of all sectoral systems. From the perspective of other policy sectors, a unified sectoral database can be used for planning purposes, risk analysis and as a support for decision-making.

Issues faced lead us back to basics: the formulation of the so called Treasury Ledger System (TLS as shown on *Figure 6*) is essential to gain proper, timely, coherent data framework in public financial accounting. An integrated PFM system should be based on a unified classification and regulatory environment in order to be sound, easily cumulated and comparable. The importance of these expectations were highlighted by the enormous effects of the sovereign debt crisis in 2008. The Council of the European Union adopted a directive [9] with regard to the budgetary frameworks of the Member States and addressed the Commission to assess the suitability of IPSAS (*International Public Sector Accounting Standards*) for the Member States.[4] The elaboration of this standard is being coordinated by EUROSTAT that studied the public accounting and auditing practices and the potential impact and sustainability of accrual accounting but its working group has not come to a conclusion yet.

The execution of the law on central government budget has a firm legislative background in Hungary. As from 2014 a new regulation entered into force that created a unique system of a combined budgetary (cash flow based) and financial (accrual) accounting, which is obligatory for all SPUs and other public sector entities. One of the main achievements was the unified chart of accounts and the detailed accounting standards set up by a government regulation[5].

Unfortunately the everyday practice is more complex since the introduction of information systems was not controlled centrally and the SPUs use separately installed accounting systems deployed in line with the specific SPU needs. Consequently developments were not settled by unified methods and sometimes the diverging requirements may aggravate the establishment of interoperable database connections.

Hungarian State Treasury – that is also the body responsible for SPU reporting – made a survey on the usage of information systems by SPUs and the compliance with legislative changes.

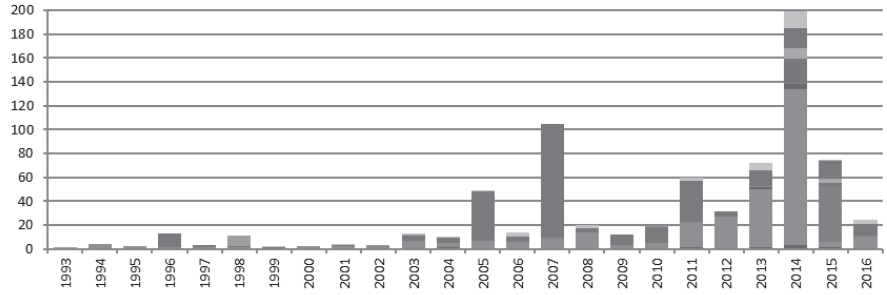

Figure 8: Year of implementation of accounting software currently in use

It was surprising that many of the 748 SPUs giving feedback did not choose to develop the current software but to change it to another, while no new supplier appeared on the market and all providers made the follow-up needed to comply with the new rules. The experiment was also interesting from the aspect of the timeliness of the developments because it took very much time to carry out the specification, procurement, development, etc. phases. Finally the following conclusions can be made:

[4] According to the latest updates his framework may be altered by the various interests of the different Member States

[5] As a reference to the survey of WBG cited above only the third of the countries apply a unified chart of accounts or accounting principles for all segments of budget execution [22].

- Parallel development – given that every SPU has to follow the same accounting standards, classifications, and rules – hinders cost efficiency.

- Moderately coordinated developments result in heterogeneity in everyday accounting and the application of the law.

As information needs are rising and adequate IT solutions are available, PFM needs to be technologically renewed in Hungary. The interoperability of existent systems serve as a fundamental basis for a sound budget execution while a central database of transactional level information provides the opportunity to analyse deeper the transfers, cash flows and performance of government entities which is planned to go forward with the help of the planned MIS project of the Hungarian State Treasury.

This paper assumes that the identified drivers of interoperability will be present in the long term and the interconnected databases will further reduce burdens improve efficiency and data quality.

6. Summary and conclusions

Interoperability is becoming a key factor of our data based economy. The spread of information technology and the digitisation of business procedures increases the need for interconnected services thus interoperability might gain a significant ground in the future. The assumption that interoperability plays a critical role in the modernization of public services and the introduction of new digital solutions is also reflected by the development strategies of the European Union.

We have seen efforts in the last decades to establish multifunctional systems – also in the field of public financial management – but these projects show very wide-ranging results. The development of data management tools is dominated by the business sector, but public sector organizations often develop their own solutions since many business-oriented solutions cannot address the specificities of the public sector. Several government ICT tools were also developed for specific tasks as separate systems that also raised the need for cooperation between them. Thus huge efforts are made towards the improvement of connectivity of these systems but the level of interoperability shows great differences also within the same organization.

It is clear that interoperability is a determining factor to meet future integrated PFM system requirements. Nonetheless, it is important to emphasize that interoperability is not a pure technological concept it has a wide range of legal, political, organizational and semantic aspects. The experience show that without the harmonization of the processes and institutional needs, the applications and technical solutions are not properly used, which effects the effectiveness and efficiency of the whole system.

Meanwhile data protection rules further accelerate the free movement of data, but it also poses new challenges to IT development. These challenges result in a demanding and fastidious mission for professionals throughout government bodies. The process going on also in public finances and a roadmap is set in favour of providing the citizens with services of a higher and higher standard. Nevertheless in Hungary the case of development policy systems and the applied comprehensive approach poses a good model for future development.

7. References

[1] ADVISORY BOARD OF THE NATIONAL COUNCIL FOR TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY, White paper on Hungarian National Data Policy, (2016)

[2] DELOITTE, First steps into the labour market. Deloitte Central Europe. (2015)

[3] DENER, C., & MIN, S. Y., Financial Management Information Systems and Open Budge Data – Do Governments Report on Where the Money Goes? Washington, DC: World Bank. (2013)

[4] DENER, C., WATKINS, J. A., & DOROTINSKY, W. L., Financial Management Information Systems / 25 Years of World Bank Experience on What Works and What Doesn't. Washington D. C.: World Bank. (2011)

[5] EUROPEAN COMMISSION, COM 72 final, "Internet Policy and Governance - Europe's role in shaping the future of Internet Governance ", (2014)

[6] EUROPEAN COMMISSION, COM 178 final, "European Cloud Initiative - Building a competitive data and knowledge economy in Europe", 19.4. (2016)

[7] EUROPEAN COMMISSION, COM 134 final, "European Interoperability Framework – Implementation Strategy ", (2017)

[8] EUROPEAN COMMISSION, National Interoperability Framework Observatory, Downloaded: 2018. 01, 30, Source: https://joinup.ec.europa.eu/collection/national-interoperability-framework-observatory-nifo?page=1

[9] COUNCIL OF THE EUROPEAN UNION, Directive 2011/85/EU of 8 November 2011 on requirements for budgetary frameworks of the Member States, (2011)

[10] EUROPEAN PARLIAMENT AND OF THE COUNCIL, Directive 2003/98/EC of 17 November 2003 on the re-use of public sector information, (2003)

[11] EUROPEAN PARLIAMENT AND OF THE COUNCIL, Decision No 922/2009/EC of September 2009 on interoperability solutions for European public administrations (ISA), (2009)

[12] EUROPEAN PARLIAMENT AND OF THE COUNCIL, Decision (EU) 2015/2240 of 25 November 2015, establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA˛ programme) as a means of modernising the public sector, (2015)

[13] EUROPEAN PARLIAMENT AND OF THE COUNCIL, 679/2016/EU regulation, General Data Protection Regulation, (2016)

[14] GOVERNMENT OF HUNGARY, Regulation No. 60/2014, a támogatásból megvalósuló fejlesztések központi monitoringjáról és nyilvántartásáról, (2014)

[15] GOVERNMENT OF HUNGARY, Resolution No. 1310/2015, a közadatok széles körű újrahasznosításához szükséges intézkedésekről, (2015)

[16] HASHIM, A., A handbook on financial management information systems for government: a practitioners guide for setting reform priorities, systems design, and implementation. Washington, D.C.: World Bank Group. (2014)

[17] INTERNATIONAL TELECOMMUNICATION UNION, Measuring the Information Society Report. Geneva, Switzerland: International Telecommunication Union. (2016)

[18] MAGYARORSZAG.HU, Új időszámítás az e-ügyintézésben, Downloaded: 2018.01.30., Source: https://hirkozpont.magyarorszag.hu/hirek/uj_idoszamitas_az_eugyintezesben.html

[19] MAGYAR ÁLLAMKINCSTÁR, Költségvetési információk, Downloaded: 2018.01.30., Source: http://www.allamkincstar.gov.hu/hu/koltsegvetesi-informaciok/koltsegvetesi-informaciok

[20] WORLD BANK GROUP, Projects of WBG, Downloaded: 2018.01.30., Source: http://www.worldbank.org/projects/search?lang=en&searchTerm=&themecode_exact=27

[21] WORLD BANK GROUP, Hungary – Public Finance Management Project (English) project Downloaded: 2018.01.30., Source: http://www.worldbank.org/projects/P043446/public-finance-management-project?lang=en

[22] WORLD BANK GROUP, Public Financial Management Systems and eServices Global Dataset, Downloaded: 2017. 12 19., Source: http://data.worldbank.org/data-catalog/pfm-systems-eservices-dataset

[23] WORLD BANK GROUP, Public Financial Management Systems and eServices Global Dataset, Downloaded: 2018.01.30., Source: http://www.worldbank.org/en/topic/governance/brief/financial-management-information-systems-fmis

CRYPTOGRAPHY CHAOS THEORY

Bulai Rodica and Victor Fanari[1]

DOI: 10.24989/ocg.v331.37

Abstract

The development of information society, which has led to an impressive increase in the volume of information, mainly economic, circulated in computer networks, accelerated the development and mostly the use of modern cryptography tools. In the last years, researchers have pointed out that there is a possible similarity between chaos and cryptography, many of the properties of chaotic dynamic systems having correlation among the cryptographic systems that are based on computational methods.

Studies carried out on chaotic dynamic systems usage in digital crypto-systems have determined the occurrence of similar to classic techniques, but also of some specific techniques and methods that have been analyzed and evaluated. The attempts to develop new encryption algorithms based on chaos theory have evolved gradually from simple solutions, which suppose the iteration of a dinamic system to obtain binary sequence used for text masking, to methods that imply coupled dinamic systems and hybrid techniques that would combine the chaos advantages with classical methods.

In this article there are presented 3 encryption algorithms based on chaos theory: RC4, Fractal Encryption and Cellular Automata, implemented in a system of encryption and operation mode analysis for each algorithm separately.

1. Introduction

The theory of chaos is one of the ways we can study nonlinear phenomena. More specifically, chaos is a state of nonlinear dynamic systems in which seemingly random events are actually predictable using simple deterministic equations. Thus, a phenomenon that seems unpredictable locally can actually be stable globally, can have well-defined boundaries and may have sensitivity to initial conditions. Small differences in the initial states can produce significant differences over time in the final states.

The theory of chaos teaches us that even very simple rules can lead to extremely complex and unpredictable behavior. Water droplet dispersion from a dripping tap is not the same if it occurs twice, even if each drop is almost exactly the duplicate of the last one. Changes in the microscopic environment have a dramatic effect on individual particle pathways in water.

Optimization problems in uncertain and dynamic environments are complex and difficult, and often classical algorithms based on dynamic programming or mathematical approaches manage to solve only small instances of problems. Attempts to develop new cryptographic algorithms based on chaos theory evolved gradually from simple solutions involving the iteration of a dynamic system to

[1] Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Str. Studentilor 7, Chisinau, MD-2012, Republic of Moldova, Tel:(37322) 509908; E-mail:rodica.bulai@ati.utm.md, fanarivictor@mail.ru

obtain the binary sequence used to mask the text to methods involving coupled dynamic systems and hybrid techniques combining the chaos advantages with classical methods.

The design and digital implementation of chaotic cryptosystems involves the use of digital chaotic functions for building flow or block algorithms.

From a technical point of view, the term "chaos" defines a particular state of a system characterized by the following:

- is never repeated (looks irregular);
- there is a dependence of sensitivity in relation to the initial conditions: extremely small differences in the values of different parameters may lead to divergent results;
- it is less ordered and can be characterized by unpredictable determinism .

Unpredictable determinism means that even a perfect chaotic system (identical motion equations and the same initial conditions) can lead to unpredictable outcomes [1].

Chaotic systems are therefore ordered, deterministic and unpredictable. It is true that "very simple" systems follow perfectly deterministic rules and yet their behavior is totally unpredictable. Deterministic, because the effects can be precisely measured and located, determining the continuation of events. Chaos, because we do not know everything that will happen, despite the fact that we know all the data that determines the events.

2. The principle of cryptography based on the theory of chaos

The principles of "chaos theory" are used to secret communications. The basic idea is that a message can be "buried" inside a chaotic signal - a sound of solar, meteorological origin, and so on. - as a screen that makes the message inaccessible to those who can not break down chaos into component elements.

Chaos-based cryptosystems use deterministic chaotic dynamic systems, either continuous or discreet, sensitive to the initial conditions. By their motion law, these dynamic systems uniquely determine the state of the cryptosystem and allow for non-catastrophic decoding of the encoded sequence. These dynamic systems are described by state functional equations (formula 1) in which a linear or nonlinear 'dynamic' ***f*** function of the system is used:

$$x+(t) = f(x(t),t) \qquad (1)$$

By ***x***, we understand the state variables vector dependent on the continuous time variable ***t***, and + represents the system state change operator.

Similarly, for discrete systems (formula 2), the state equation is written according to the discreet variable of time ***n*** in form:

$$x[n+1] = f(x[n],n) \qquad (2)$$

It is preferred to use non-linear dynamic systems that may have more than one set of boundaries in a permanent regime, with different attraction bases, very dependent on the initial condition, so that long-term prediction of their condition becomes impossible.

In the case of mixed discrete chaotic cryptosystems, the encryption and decryption procedure is performed by multiple, inverse and direct iterations, and the encoded sequence corresponds to the number of iterations performed. These systems prove to be particularly robust against statistical attacks.

The principle of cryptography based on the theory of chaos is given by the diffusion and confusion of trajectory parameters generated on the basis of the encryption key and the transmitted message. With small variations of the transmission key, extreme changes of the phase path trajectory for the dynamic system used must occur. This ensures the cryptosystem resistance against raw attacks based on the testing of all possible transmission keys.

Chaotic trajectories are neither periodic nor quasi-periodic, and they have a random appearance with a "white noise" (wideband) power spectrum [2].

No computer or software can predict the trajectory of a chaotic dynamic system, because the algorithmic complexity of the trajectories is positive, given by the Kotulski-Szczepanski entropy of the system. This is based on the idea of designing efficient data encryption techniques based on the theory of chaos so that the entropy of the system grows through coding and exceeds the computational capabilities of the cryptanalyst.

Optimization of encryption algorithms aims at reducing data processing time, reducing memory capacity, diversifying potential transmission keys, and decreasing the efficiency of cryptographic attacks. Applying a precision to compress the information source to reduce its redundancy reduces the risk of interception of the transmission key and the effectiveness of any attack.

The value of a cryptosystem is appreciated on the basis of several factors: degree of secretion, encryption key size, error propagation, uniqueness distance.

Developing a powerful cryptosystem involves maximizing the amount of work required for cryptanalysis by any method. When the cryptanalysis of an encryption algorithm is performed, the general assumption is that the cryptanalyst knows exactly how the cryptosystem works.

3. Ciphering and deciphering methods of chaotic cryptographic systems

There are two ways to use chaos to encrypt information.

The add-on method consists of separately creating the chaotic system and the information and then adding the two signals. In turn, the interlocutor has the system keys (initial conditions and system equations sent in advance) with which he can in turn create a chaotic system like the one from the broadcast. When he receives the additional message of the chaotic system, he has nothing to do but recover the message by extracting the "mask".

The inclusion method not only drowns in the chaos of the message, it is even deep inside the structure of the chaotic system, still a hindrance for a spy in his attempt to decipher the message.

The message is therefore not transported by the chaotic wearer through the transmission line, but it is its own bearer. This line only contains the transmitter data that will allow the recipient to discover the transmitted message.

The difference between the addition and inclusion methods is that in the latter case the message is not "retrieved" in the receiver but is "reconstituted" by the receiver.

Attempts to develop new cryptographic algorithms based on chaos theory evolved gradually from simple solutions involving the iteration of a dynamic system to obtain the binary sequence used to mask the text to methods involving coupled dynamic systems and hybrid techniques combining the chaos advantages with classical methods.

The most promising encryption systems based on chaotic dynamic systems have proven to be the ones using linear functions on portions. The discrete representation of the chaotic system values can lead to the loss of intrinsic properties of the continuous dynamic systems, appearing problems related to the dynamic degradation of the behavior of digital chaotic functions [3].

By using simple disruptive methods, good performance can be achieved for the chaotic digital functions used to implement random (pseudo) sequence generators, but also for building encryption algorithms.

The development and implementation of an encryption algorithm pursues aspects related to the provision of chaotic features throughout the entire system operation period. For this purpose, rules were used to define the dynamic system's initial parameter and condition to fully exploit the key's size and to ensure sensitivity to its modification. Obtaining a real-time workflow for real-time applications is determined both by the implementation mode used for chaotic dynamic systems and by the way the algorithm is defined, which is why it has been proposed to use a number of fixed iterations of small size, but determined by the key, through a very sensitive relationship to changes [4].

The approach to many variants of chaos-based encryption algorithms has so far been limited to software, primarily due to ease of use, enhancement, portability and flexibility. But with technological development and increased demands on high-speed work and key safety, hardware implementations become more suited both in terms of physical security and encryption / decryption speed.

By implementing chaotic generators and encryption system, it has been demonstrated that digital hardware structures can be used with good performance to protect information using chaos- specific techniques.

4. Analyzed cryptographic systems based on the theory of chaos

Three algorithms based on chaos theory have been selected and analyzed: RC4 (Rivest Cipher 4), Cellular Automata and Fractal Algorithm, which are part of a stream cipher system and have been integrated into a single encryption entity and Decryption.

4.1. The *RC4* algorithm

Rivest Cipher 4 is a flow cipher. While it's remarkable for its simplicity and speed in software, more vulnerabilities have been discovered, making it unsafe. RC4 is the most commonly used cipher-

stream software in protocols such as SSL or WEP. Unfortunately, RC4 does not meet the current high security standards and some methods of using it lead to very unsafe cryptosystems.

The cipher consists of two major components, the Key Scheduling Algorithm (KSA) and the Pseudorandom Generation Algorithm (PRGA). The internal state of RC4 contains a permutation of all 8-bit words, i.e., a permutation of N = 2^8 = 256 bytes, and the KSA produces the initial pseudorandom permutation of RC4 by scrambling an identity permutation using the secret key k. The secret key k of RC4 is of length typically between 5 to 32 bytes, which generates the expanded key K of length N =256 bytes by simple repetition. If the length of the secret key k is l bytes (typically $5 \leq l \leq 32$), then the expanded key K is constructed as K[i] = k[i mod l] for $0 \leq i \leq N-1$. The initial permutation produced by the KSA acts as an input to the next procedure PRGA that generates the keystream (Figure 1).

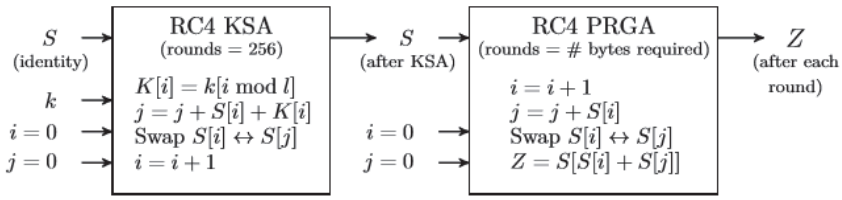

Figure 1: Description of RC4 stream cipher [5]

For round r = 1,2,... of RC4 PRGA, we denote the indices by i_r,j_r, the keystream output byte by Z_r, the output byte-extraction index as $t_r = S_r[i_r] + S_r[j_r]$, and the permutations before and after the swap by S_{r-1} and S_r respectively. After r rounds of KSA, we denote the state variables by adding a superscript K to each variable. By S_0^K and S_0, we denote the initial permutations before KSA and PRGA respectively. The S_0^K 0 is the identity permutation and $S_0 = S_N^K$ is the permutation obtained right after the completion of KSA[5].

4.2. The *Cellular Automata* algorithm

Proposed by John Conway, as "The Game of Life", played on a grid, divided into cells. Each cell can be "live" or "dead," and a set of four rules determines whether any given cell will live, die or be born at each iteration. The simple set of rules of the game has led to surprisingly complex and convincing behavior, and a new field of research called "Cellular Automata" has emerged around.

One interesting point that can be extracted from this area is that any simulation of cellular automates, no matter how complex they are, is completely determined by the state of starting the cells on the grid.

The *Cellular Automaton* algorithm is currently not widely deployed, such as the *RC4* algorithm. Most often it is used in image encryption, as it provides the user with a variety of encryption methods. There are some useful aspects to this: from a single configuration of cells in a grid, a huge volume of unpredictable and complex information can be built. After a thousand generations, who could predict which cells would be active without knowing the initial state and without running the whole simulation? If a single cell was different in the initial configuration, after sufficient generations, the condition of each cell will ultimately be different (Figure 2).

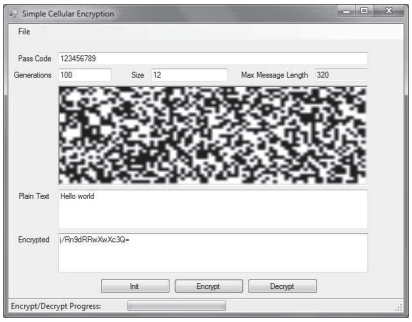

Figure 2: Automated Cellular Algorithm

Generating pseudo-random numbers through Cellular Automats.

Cellular automata are dynamic systems where space and time are discreet. A CA (Cellular Automated) consists of a series of cells, each of which can be in one of a finite number of possible states, updated in a discrete time synchronously, according to a local and identical rule.

Consider only Boolean automata for which the cellular state is $s \in \{0, 1\}$.

The condition of a cell at the next time step is determined by the current state of a neighborhood around the cells. Cellular matrix (grid) is d-dimensional, where d = 1, 2, 3, which are used in practice. In our case d = 1 and d = 2, that is a one- and two-dimensional grid. The same rule contained in each cell is essentially a finite state, usually specified as a rule table (also known as the transition function), with an entry for each possible neighborhood of configurations. Neighboring cell of a cell is formed by its own state and neighboring cells (adjacent) [6].

For unidimensional CA, a cell is connected to a local neighbor r (cell) on each side, where r is called radius (so each cell has 2r + 1 neighbors). For two-dimensional CA, two types of cellular districts are usually considered: 5 cells, consisting of its own cell together with the four non-Dionygon evecs (also known as von Neumann neighborhood) and 9 cells, consisting of its own cell with The eight surrounding neighbors (also known as the Moore neighborhood). When a finite dimensional grid is analyzed, periodic spatial conditions are frequently applied, resulting in a circular grid for the unidimensional case, and the toroidal grid for the two-dimensional case.

S. Wolfram first proposed CA one-dimensional as a pseudo-random number generation (PRNG). In particular, he extensively studied the bit sequences generated by rule 30 in his numbering scheme for unidimensional, r = 1 rules, if the rule number represents the decimal format of the binary coding number in the rule table.

In Boolean format, Rule 30 can be written as in Formula 3:

$$s_i(t + 1) = s_{i-1}(t) \text{ XOR } (si(t) \text{ OR } s_{i+1}(t)) \qquad (3)$$

where s_i (t) is the state of the cell *i* at time *t*. The formula gives the state of the cell *i* in time step *t* + *1* as a boolean function of the states in the vicinity of the cells at time *t*. Pseudo-random bit sequences are obtained by sampling the values that a particular cell (usually the central one) touches as a function of time [7].

An uneven randomizer was presented consisting of two rules, 90 and 150, arranged in a specific order in the grid (Figure 3).

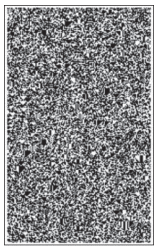

Figure 3: Random Number Generator uneven unidimensional

In the boolean form, rule 90 can be written as:

$$s_i(t + 1) = s_{i-1}(t) \text{ XOR } s_{i+1}(t) \quad (4)$$

and rule 150 can be written as:

$$s_i(t + 1) = s_{i-1}(t) \text{ XOR } s_i(t) \text{ XOR } s_{i+1}(t) \quad (5)$$

Generating a string of numbers based on cellular automata.

Let P be a clear message and E is a cipher algorithm. Fundamental transformation to get C-chipherd text is therefore:

$$C = E_k (P) \quad (6)$$

where k is the key of transformation that distinguishes a particular encryption in a transformation family using the same decryption algorithm. To recover the original message, a D_k decryption function using the same key is defined as the inverse of E:

$$P = D_k(C) = D_k(E_k(P)) \quad (7)$$

Encryption algorithms that operate with clear text on a single bit at a time are called flux cipher algorithms. A flow cipher breaks the P message into a bit stream or successive bytes $p_1, p_2, ..., p_q$ and encrypts each pi with a bit stream (or bytes) $k_1, k_2, ..., k_q$ generated by a key generator so that:

$$E_k (P) = E_{K1} (p_1) E_{K2} (p_2) \quad (8)$$

A common encryption operation used is the XOR-exclusive operation:

$$c_i = k_i \text{ XOR } p_i \quad (9)$$

where c_i is the i-th bit of the cipher text. Applying the same operation on cipher text allows recovery of the original text:

$$p_i = c_i \text{ XOR } k_i = (k_i \text{ XOR } p_i) \text{ XOR } k_i \quad (10)$$

4.3. The *Fractal* algorithm

The *Fractal* Algorithm uses the famous *Mandelbrot* fractal to convert the encryption key (provided by the user) to a longer key, which is then XORed with the clear text, resulting in encrypted text.

Many famous encryption algorithms extend to some extent the encryption key and then, after moving, move and replace the bits in plain text, they use the XOR operation with the extended password, and this process is usually repeated a number of times.

The *Fractal* Algorithm tries to create a random key extended using the Mandelbrot fractal instead of using a fixed rule [8].

Moreover, the *Fractal* algorithm encrypts the entire file as a single large block instead of encrypting it divided into blocks of 256 bits, so it does not use the same encryption key on each block but uses only one large encryption key to It encrypts the entire text (which should mean fewer repetitions - fewer chances of attacking successfully).

Although it is more complex than the other two algorithms, *Fractal* is used in encryption of visual images, and, at the same time, the encryption information using its iterating.

Principles of Fractal Encryption Algorithm.

Encryption is the repetition of binary operations inside a loop, between which the fractal encryption key is calculated [9].

Suppose we have a series of messages *M(j)* for $j = 1$ up to N, we want to send safely to the recipient. We will need a reversible encryption function E:

$$E(M(j), k) \dashrightarrow X(j) \quad (11)$$

where k is an encryption key and *X(j)* is the properly encrypted message. Then the message is sent to our receiver, which has a complementary function E' to decrypt the encrypted message:

$$E'(X(j), k) \dashrightarrow M(j) \quad (12)$$

However, both *E()* and *E'()* function can not be performed using Fractals. On the other hand, there are some functions, such as XOR (or-exclusive) that are their own complementaries:

$$(M(j) \text{ XOR } k) \dashrightarrow X(j) \quad (13)$$

$$(X(j) \text{ XOR } k) \dashrightarrow M(j) \quad (14)$$

But *XOR* is also a weak encryption function, and although it is perfectly sure of a single message, but if we use it more than once with the same key *(k)* it becomes very easy to perform reverse engineering, thus making the operation Unsure *XOR* for single key encryption systems. This can be solved by using another key at each iteration:

$$M(j) \text{ XOR } K(j) \dashrightarrow X(j) \text{ și } X(j) \text{ XOR } K(j) \dashrightarrow M(j) \quad (15)$$

Most often we want to generate a series of identical keys on both sides: sender and receiver. But we must be able to generate a series of keys that are secure in cryptography. That is, even if an external observer knows all of the previous keys, he would not be able to predict the next key in the series with precision. And because we'll need a different set of keys each time, in fact, we need actual serial key to the basic key [10].

The solution is to use *a Master Key - MK*, and another *H*-encryption function, to generate the specific keys for each message:

$$H(MK, j) \dashrightarrow K(j);\ M(j)\ XOR\ K(j) \dashrightarrow X(j) \text{ și } H(MK, j) \dashrightarrow K(j);\ X(j)\ XOR\ K(j) \dashrightarrow M(j) \quad (16)$$

In this case fractals are used, because as we can see above, the H function does not need a complementary function *H'*. So we can freely use a basic *Fractal* function with a master key to generate the local key series [11].

5. Security and performance of algorithms usage

Unlike a modern stream cipher (such as eSTREAM), *RC4* does not take just one random number (nonce) along with the key. This means that if a single long-term key is used to safely encrypt multiple streams, the protocol must specify how to combine this arbitrary number (nonce) and the long-term key to generate the key flow for RC4. To address this operation, it is necessary to generate a "fresh" RC4 key by hashing a long-term key with a nonce. However, many applications that use RC4 simply hook the key and nonce.

Because the RC4 is a flux cipher, it is more malleable than the common block ciphers. If it is not used along with a strong message authentication (MAC) code, then encryption is vulnerable to a bit flipping attack. The method is vulnerable to a stream cipher attack if it is not implemented correctly. Moreover, the double encryption of a message with the same key may accidentally decrypt the encrypted text, since the involuntary nature of the XOR function would result in the second operation inversion of the first.

If the keyflow of the Cellular Automation algorithm is truly unpredictable, then we have the so-called «one-time pad», the system that is perfectly safe (assuming the keys are not stolen). The one-time-pad system was invented by J. Mauborgne, and is based on a variation of the Vernam cipher in which the key is not repeated. However, the encryption system is impracticable because the sender and receiver must be in possession and protect the random key. In addition, the total amount of data that can be encrypted is limited by the key length available.

Thus, the security of a flow cipher system, of the given algorithm, is based on the predictability of bits in the key stream. A good pseudo-random statistic of the key stream is not enough in cryptographic applications: a perfect RNG may be completely inappropriate if the next random bit can be predicted from the previous sequence. From this point of view, ACs are more appropriate than classical RNGs, which are very easy to break, taking into account the given algorithm and a small portion of the sequence.

By analyzing the performance of these encryption and decryption algorithms, after the required time (seconds) for encrypting a data volume (number of characters), then we can mention that the Fractal algorithm requires the smallest time, regardless of the amount of encrypted (figure 4) or decrypted (figure 5) information.

For developing these 3 algorithms we used C# language - no additional libraries - just standard functions and standard "Windows Form" compiler (used in Visual Studio). We used random characters (numbers / letters / signs). The maximal length that we used is 500.000 characters. Cause as you can see from the diagram, RC4 algorithm is taking much more time to do all the stuff in the background (almost 350 seconds).

First of all, we started with 1000 characters - and as you can see the encryption and decryption is around 0-2 seconds. After this, we started to increase the number of characters to see what is the difference between these algorithms (RC4, Cellular Automaton, and Fractal). So as you can see from the graph - Fractal algorithm is less affected by the length of the encrypted text. And for 100000-500000 characters it can take a long time to encrypt/decrypt for RC4 and Cellular Automaton. This is caused by the fact that it needs to know the value for each "neighbor". Startup time is almost the same for all these algorithms, but as we go with a multi characters text, the most efficient is Fractal of course.

All these algorithms are using the physical memory to do all the encryption/decryptions and to generate all pseudo-random numbers and they are using also the CPU to maintain a fast solution for the end user.

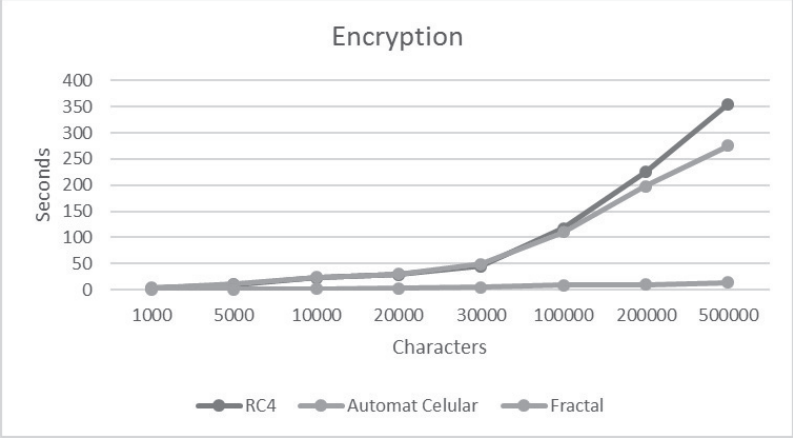

Figure 4: Encryption Performance

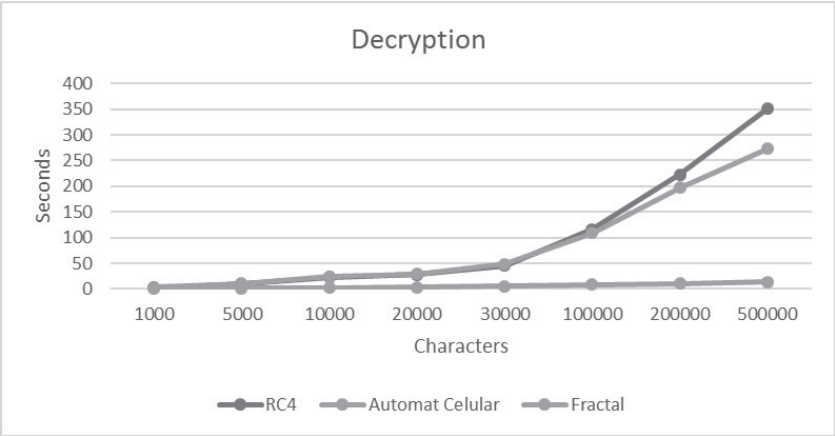

Figure 5: Decryption Performance

6. Conclusions

Studies on the use of chaotic dynamic systems in digital cryptosystems have led to the emergence of similar techniques to classical ones, but also to specific techniques, methods that have been analyzed and evaluated. Attempts to develop new cryptographic algorithms based on chaos theory evolved gradually from simple solutions involving the iteration of a dynamic system to obtain the binary sequence used to mask the text, to methods involving coupled dynamical systems and hybrid techniques combining the chaos advantages with classical methods.

The application of chaotic dynamic systems in the development of new cryptographic algorithms is in the process of development along with the technological evolution. Many of the proposed methods are still in their early stages, due to the relatively slow implementation technology and insufficient cryptographic resilience, but it should be noted that chaos can be a source that could be exploited to obtain robust cryptosystems for attacks based more and more on the high calculation ability of the new performance processors.

By enrolling in the attempts made to exploit the intrinsic characteristics of chaotic dynamic systems, cryptography based on the theory of chaos constitutes a new direction of research in the field of data protection in the last period. Studies conducted in this direction were followed by the proposal of specific solutions for the use of dynamic systems with chaotic behavior for the realization of robust and secure communication systems. Pseudo-random generators, block ciphers, and hash functions are three of the best-known security service delivery methods in which chaos-based solutions have been proposed.

The development and implementation of an encryption algorithm pursues aspects related to the provision of chaotic features throughout the system's operating period. Obtaining a working speed for real-time applications is determined by both the deployment mode used for chaotic dynamic systems and the way the algorithm is defined, which is why it has been proposed to use a number of fixed iterations of small size, but determined by the key, through a very sensitive relationship to changes.

By using simple disruptive methods, good performance can be achieved for the chaotic digital functions used to implement (pseudo) random sequence generators, but also for building encryption algorithms.

The present work, through modeling, simulation and, in particular, through the concrete implementation of digital chaos based cryptographic systems, has attempted to respond to new trends by proposing specific solutions and presenting the results obtained.

7. References

[1] MOGOLLON, M., Cryptography and Security Services: Mechanisms and Applications, New York, Cybertech Publishing, 2008, 26-27.

[2] KONHEIM, A. G., Computer Security and Cryptography, John Wiley & Sons, Inc., 2007, 99, 350.

[3] MAO, B., Современная криптография (теория и практика), М.: Вильямс, 2005.

[4] BREDIN, S., Chaos theory and Cryptography, https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxicmVkaW5jcnlwdG8yfGd4OmRkZmRlOWVhNmFkMThjYg

[5] GUPTA, S. S., Analysis and Implementation of RC4 Stream Cipher, Indian Statistical Institute, India, 2013.

[6] WOLFRAM, S., Cryptography with Cellular Automata, http://www.stephenwolfram.com/publications/academic/cryptography-cellular-automata.pdf

[7] HENRIQUES, M. A. A., New Possibilities for Cellular Automata in Cryptography, http://www.criptored.upm.es/cibsi/cibsi2011/info/Ponencias/5.%20New%20Possibilities%20for%20Cellular%20Automata%20in%20Cryptography.pdf

[8] AL-AKAIDI, M., Fractal Speech Processing, http://assets.cambridge.org/97805218/14584/frontmatter/9780521814584_frontmatter.pdf

[9] Fractal-Based Encryption, http://www.techbriefs.com/component/content/article/ntb/tech-briefs/photonics/2579

[10] GUPTA S., BANSAL, N., Image Encryption Techniques using Fractal Geometry, http://www.iosrjournals.org/iosr-jce/papers/Vol16-issue5/Version-1/F016513135.pdf

Internet and Society

THE PERMANENT CAMPAIGN IN SOCIAL MEDIA: A CASE STUDY OF POLAND

Dorota Domalewska[1]

DOI: 10.24989/ocg.v331.38

Abstract
New media technologies provide new venues for political communication enabling politicians to wage a permanent campaign. Participatory platforms have paved the way for new forms of political communication during non-election period when those seeking or holding office can increase media coverage, create their public image and foster deeper relationships with the public. The purpose of the paper is to contribute to the discussion on permanent campaign; specifically, the study focuses on presenting the method of embracing new media technologies (in particular Twitter) by politicians' during a non-election period in Poland. The analysis aims to investigate online activity, the design of Twitter profiles and the implementation of campaign-like techniques by the politicians. The findings shed light on the Polish MPs' application of participatory platforms as a tool of strategic communication used to increase media visibility, and share messages across in a one-way communication.

Keywords*: social media, Twitter, permanent campaign, political communication, political marketing strategies*

1. Introduction

Social media have led to a major shift in the way political campaigns are run and won. Social networking sites provide new venues for campaigning, debates and activism. Not only do new actors, such as political bloggers and activists, take an active role in the public discourse but also politicians post, share and comment current events as they are unfolding. Social media have paved the way for new forms of political participation that never before existed [1] where individual politicians can increase their media exposure [15], ensure contact with their electorate [19] and boost popularity during both election and non-election periods thus allowing for permanent campaign to take place.

The present paper investigates online political communication of Polish MPs during non-election period. In particular, active Twitter accounts of all members of the lower house of the Polish parliament (N=460) were analyzed in order to answer the following research questions: (1) How do MPs build their Twitter profile?; (2) Which campaign-like techniques do MPs implement on Twitter? In order to answer the research questions, content analysis of MPs' Twitter accounts has been performed. The aim of the analysis was to investigate the politicians' use of new media technologies. The study focused on design, online presence, and political marketing strategies employed by politicians.

[1] War Studies University, Faculty of National Defence, Warsaw, Poland, d.domalewska@akademia.mil.pl

2. Permanent campaign in Poland

The contemporary politics has taken the form of permanent campaign where media coverage and public popularity have become the unswerving focus of politicians thus turning governing into campaigning [4]. Thus, permanent campaign involves "adopting the campaigning style of governing to retain or even increase [politicians'] popularity, motivated by the institutional, political, and technological evolutions including mainly the decline of parties, the rise of television, and the advent of new political technologies" [14].

When the distinction between campaigning for national office and holding office becomes vague, several features increase in importance: strategic calculation involved in public image creation, building public support [25], growing interest in opinion polls [21, 22], policy contestation, extensive media exposure [27], focus on fund-raising [7] and media preoccupation with popularity of individual politicians. Opinion polling and resorting to professional campaign consultants have begun to shape political strategy during non-election periods because it is one of the most reliable tools that reveal citizens' opinion, interests, attitudes, preferences, approvals and prejudice the knowledge of which helps to gain electoral success. President Bill Clinton used market research and public relations memos to maintain public support [10], Barack Obama turned to pollsters for advice on developing more persuasive strategies [22] whereas Tony Blair employed market research analysts from the US who advised him on communication strategies and to keep track of popularity ratings [21].

At the permanent campaign age, maintaining popularity has become a key focus of major politicians holding office. Media coverage is one of the elements that can help to win popularity. Politicians have at their disposal several tools they willingly use to step into the spotlight; for example, they might share personal stories, which turns politicians into celebrities. Antagonism and multi-dimensional conflict are other ways that increase media visibility. Thus, constant image making as well as a struggle for visibility and unswerving popularity have become increasingly important in today's digital age.

3. Social media – a permanent campaign instrument

Politicians eagerly use Internet-based tools (such as websites, e-mail, forums) and social media to get their message across. In particular, social media have become a popular instrument of creating positive public image and boosting popularity of individual politicians not only due to low cost and expected broad reach [17] but also owning to innumerable benefits: ease of sharing information, mobilizing citizens, and fund-raising [8]. Politicians can easily bypass media gatekeepers and refer directly to citizens, social media users. Traditional mass media tend to favour major political actors and adhere to a predetermined political or ideological line of the publishing house [15] whereas posting messages or tweeting provides politicians with an additional option to access and shape information. The internet increases the visibility of small and fringe parties, thus becoming a free marketing tool [24], which political actors make use of to step into the spotlight or presenting unfavourable events in a favourable light. Politicians select information to be posted, take autonomous decisions on creating their profile, and build self-controlled authenticity [18]. Thus, social media users get up-to-date news stimulating their attention, which is both an ingredient of marketing communication and an element of the permanent campaign. Social media users become spectators of the political drama evolving in front of their eyes, which on the one hand keeps them glued to their mobile device and on the other hand could lead to information chaos [20].

In Poland, the Internet became the arena of political campaign for the first time in 1997 during the parliamentary campaign. At that time first websites and chats of the political parties taking part in the campaign were developed [3] and campaign ads were shared in the new media (mainly YouTube) [2]. Websites make convenient platforms for sharing content (e.g. election programmes, politicians' profiles, current news, etc.) delivered through attractive design that aims at creating a credible and stable image [16]. Websites are interactive in nature (e.g. discussion forum, chat), which is engaging for citizens and helps to form a virtual community. However, at present politicians tend to turn their websites into a notice board: they only share and update information but fail to provide any feedback [6]. A study carried out by Ward et al. [26]shows that less than a third of the websites run by political parties in the UK enables citizens to share their opinions in online forums, chats, or provide another form of interaction. Similarly, in Poland political parties fail to make use of the websites' possibility to form a virtual community [16]. Even if a website offers a discussion forum, it usually does not perform its primary function, namely two-way communication with citizens and political discussion.

Social networking platforms have changed the nature of political communication. They have become a popular political marketing tool; due to the potential symmetrical and real time nature of communication social media facilitate building relations and increasing engagement. However, one-way communication prevails when a great number of politicians enthusiastically post messages and tweet, but rarely comment them [26], which resembles traditional though independent media. Despite limited interaction between political actors and social media users, it is social media, not self-hosted websites, that have become platforms where campaign-like activities are carried out. Social networking sites enable politicians to select the content and time they update their status or tweet. Moreover, every tweet or post can include a hyperlink to a website. On average every fourth tweet in election campaign in Australia in 2010 [5] and in Belgium in 2012 [9] redirected users to a website of mainstream media or another social platform (Twitter, YouTube, blogs, Instagram, Facebook and other). Most frequently the hyperlinks were shared alongside a photograph, which proves the advantage of visual over graphic content. Numerous studies have proved that online presence has had a positive impact election results in Brazil [12], in Turkey [23], in Australia [11], and the US [8]. Few studies point at the limited effect of online campaigning; for example, Hansen and Kosiara-Pedersen [13] found that using online tools correlates with election results of same-party candidates rather than inter-party competition.

Politicians use several permanent campaign strategies during non-election periods. First, building trust is a fundamental marketing strategy that facilitates forming a relationship with a customer or electorate. Politicians develop trust when they are transparent, react to feedback, explain adequately so that all ambiguities and understatements are resolved. Politicians should convey an impression of a credible and pleasant personality. Furthermore, trust can be developed through direct contact. New media users differs significantly from the mass consumption consumers in that they want to be treated individually. To meet this demand, marketing companies make use of a variety of online tools that scan new media users' online behavior in order to offer them personalized content. Finally, it is vital to establish a regular contact with users. Politicians should react to users' messages and challenge them rather than merely post media statements.

4. Research methodology

Taking into consideration the impact social networking platforms have on political communication, the present study focuses on MPs' use of social media, in particular Twitter, to communicate with the public during non-election periods. The following research questions were addressed in the

study: (1) How do MPs build their Twitter profile? (2) Which campaign-like techniques do MPs implement on Twitter?

The present study draws on data collected from all members of the lower house of the Polish parliament who had an active Twitter account at the time of data collection, i.e. August-September 2017. Out of 460 MPs holding office at a lower house, the Sejm, 238 have active Twitter profiles. The analysis was carried out in several steps. First, Twitter analytics tools were used to evaluate Twitter data (such as a number of tweets, retweets, followers). Next, each Twitter account was analyzed using Content Analysis technique, which helps to gain systematic, objective and quantitative analysis of data. Observations were recorded in a schedule with predetermined categories which focused on examining in detail the design, online presence, and political marketing strategies employed by the politicians.

5. Results and discussion

Design of a Twitter profile is the first factor that projects the user's identity; that is why, both politicians and professional campaign consultants expend considerable effort to organize the profile page so that it presented the politician properly, generated more traffic and increased visibility. The effective use of color, profile and header picture, as well as aesthetic appeal are factors that create the first impression whereas the user bio, infinitely scrollable timeline of the user's tweets, videos, photos, and shared tweets build the user's personal brand.

The analysis of the MPs' profile picture shows that most politicians (97%) select a formal head and shoulders portrait photograph in smart outfit, which creates an impression of a competent and compelling professional. Not many politicians display a photograph of themselves with their spouse or other citizens; few politicians upload a photograph of an object (emblem, horse or an abstract image). The selection of the header photograph is done in a more varied way, which is presented in Figure 1.

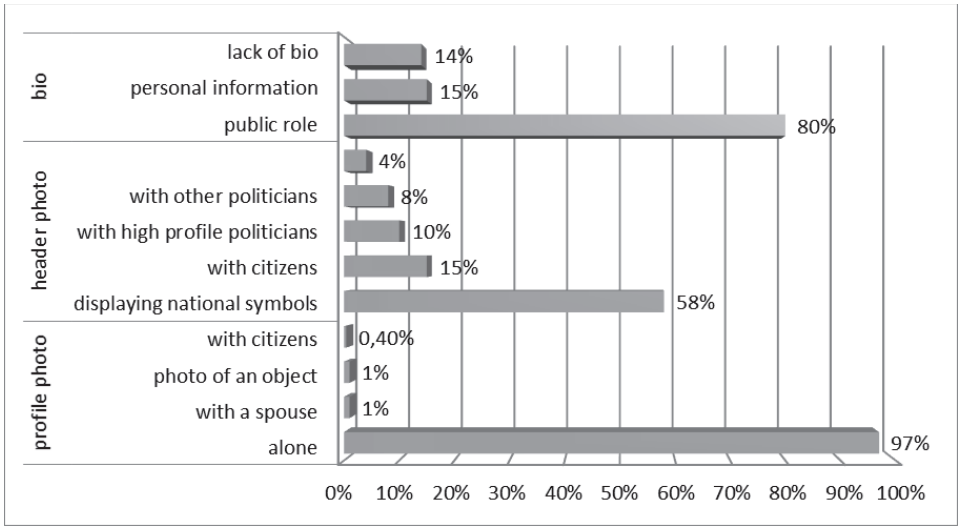

Figure 1: Strategies used to build a Twitter profile

Most MPs display a symbol in their header photo: national symbols, party identification (including a number of key words or hashtags, i.e. social or political priorities the MP stands for) or a landscape (most frequently a city landscape). Others set a header photo presenting other politicians or citizens. A great number of politicians include a short bio that mostly discusses their public roles. Few politicians opt for sharing personal information about their family, education or hobby. Thus, Twitter accounts of the MPs are mainly used as an alternative method of presentation the politician profile in the formal context.

The three elements of a Twitter profile: profile photo, header photo and bio give a hint of the user's identity. Clearly, the Polish MPs intend to create a professional image: through the selection of photographs they project themselves as competent politicians who cooperate with other politicians and perform their constituency roles. Needless to say, the content is carefully selected to display their professionalism (photographs with citizens and other politicians, a bio showcasing their duties), values (header photograph including national or party symbols as well as slogans that emphasize their priorities), and approachability (family photographs, a bio revealing their hobby).

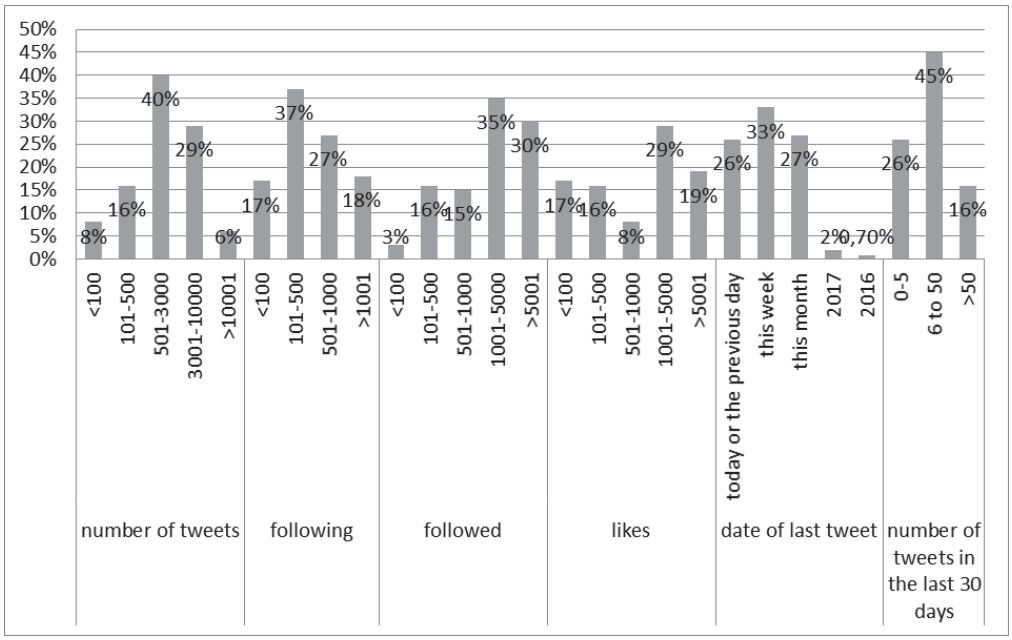

Figure 2: The MPs' activity on Twitter

The findings displayed in Figure 2 clearly show that the MPs are rather observed that observing other profiles. Undoubtedly, high-profile politicians attract the greatest number of observers. This finding proves that, on the one hand, Twitter is an instrument used by politicians to get their message across to both the electorate and the media. Thus, they use Twitter as a word-of-mouth instrument, but the limited number of accounts they follow proves that they do not listen to other messages very attentively. On the other hand, the MPs massively share tweets posted by other politicians or the media rather than tweet original content, which is both easier and less face-threatening than, but still serves the main purpose: stepping into the spotlight. Posting a content tweet requires in-depth analysis and responsibility (all tweets can be potentially widely

commented). At the same time, it ensures online visibility, which is of utmost importance. Thus, in both cases, Twitter is used as a tool that increases media coverage. Furthermore, the tweets that are most frequently shared are repetitive and predictable: the MPs publicize media coverage of important events, inform about their presence in traditional media, present results of their work, and reproach their political opponents.

Finally, a great number of politicians (21%) present the results of polls whose aim is to prove popularity of individual politicians, parties, or actions (members of the ruling party present research results to prove effectiveness of their reforms whereas members of the opposition publicize statistics to prove the contrary). Thus, opinion polling has been widely used during non-election periods in order both to ensure the politicians' public support and to bring the opposition into disrepute.

6. Conclusions

Politicians incorporate social networking platforms into their strategic communication with the public due to their low cost and expected broad reach. Social media have become an invaluable tool that helps to fulfil several objectives: reaching and mobilizing general public, increasing media visibility, ensuring online presence, building popularity, and creating positive public image. The research proves that social media have become an integral part of governing that facilitates political communication on the national level. First, each MP's profile is created paying close attention to detail: the effective use of colour, profile and header photograph, bio, and aesthetic appeal. The politicians in Poland are presented as competent and persuasive professionals who cooperate with other politicians, perform their constituency roles, cherish a set of values and are approachable. Not many MPs upload photographs of their family nor share private information. A common strategy is to post a symbol in their header photo, most frequently national symbols, party identification (including a number of key words or hashtags, i.e. social or political priorities the MP stands for) or a landscape.

Furthermore, the Polish politicians holding parliamentary power tend to rely on sharing tweets rather than updating their profiles with original tweets and are followed rather than following other profiles. This finding proves that the MPs use participatory platforms to increase media visibility and share their message across in a one-way communication. Finally, they frequently display the results of opinion polls, mainly with the aim to prove their popularity or to bring the opposition into disrepute.

7. References

[1] ANDUIZA, E., CANTIJOCH, M. & GALLEGO, A., Political Participation and the Internet -- a Field Essay. Information, Communication & Society, Vol 12, No 6, pp. 860 – 878, 2009.

[2] ANNUSEWICZ, O., Celebrytyzacja Polityczna, in: Studia Politologiczne, 20, 268-278, 2011.

[3] BISKUP, B., Komunikowanie Polityczne w Tradycyjnych i Internetowych Serwisach Informacyjnych – Analiza Przejawów Kultury Politycznej przed Wyborami Prezydenckimi w Polsce w 2010 Roku, in: Studia Politologiczne, 26, 109-131, 2011.

[4] BLUMENTHAL, S. L., The Permanent Campaign: Inside the World of Elite Political Operatives. Boston, Beacon Press 1980.

[5] BRUNS, A., and BURGESS, J., #ausvotes: How Twitter Covered the 2010 Australian Federal Election, in: Communication, Politics and Culture, 44(2), 37, 2011.

[6] CASTELLS, M., The Internet Galaxy: Reflections on the Internet, Business and Society, New York, 2002.

[7] CORRADO, A., Running Backward: The Congressional Money Chase, in: N. Ornstein and T. Mann (eds), The Permanent Campaign and its Future, Washington DC: American Enterprise Institute and the Brookings Institute, pp. 75-107, 2000.

[8] DAVIS, R., BAUMGARTNER, J. C., FRANCIA, P. L., and MORRIS, J. S., The Internet in US Election Campaigns, in: Routledge Handbook of Internet Politics, 25-39, 2009.

[9] D'HEER, E., and VERDEGEM, P., An Intermedia Understanding of the Networked Twitter Ecology, in: B. Pătruţ, M. Pătruţ (eds) Social Media in Politics, Springer, Cham, 81-96, 2014.

[10] EDWARDS, G., Campaigning is not Governing: Bill Clinton's Rhetorical Presidency, in: C. Campbell and B. Rockman (eds) The Clinton Legacy, London, 33-47, 1999.

[11] GIBSON, R. K. and MCALLISTER, I., Does Cyber-campaigning Win Votes? Online Communication in the 2004 Australian Election, in: Journal of Elections, Public Opinion and Parties, 16(3), 243-263, 2006.

[12] GILMORE, J., Ditching the Pack: Digital Media in the 2010 Brazilian Congressional Campaigns, in: New Media and Society, 14(4), 617-633, 2012.

[13] HANSEN, K. M., and KOSIARA-PEDERSEN, K., Cyber-campaigning in Denmark: Application and Effects of Candidate Campaigning, in: Journal of Information Technology and Politics, 11(2), 206-219, 2014.

[14] HECLO, H., Campaigning and Governing: A Conspectus, in: N. Ornstein and T. Mann (eds) The Permanent Campaign and its Future, Washington, 1-37, 2000.

[15] JEZIŃSKI, M., Po co Politykom Nowe Media? O Politycznym Istnieniu w Wirtualnej Przestrzeni, in: Nowe Media. Czasopismo Naukowe, 2, 11-30, 2011.

[16] KANCIK, E., Budowanie Wizerunku – Strony Internetowe Polskich Partii Politycznych, in: M. Wincławska (ed.) Partie Polityczne w Początkach XXI Wieku. Problemy Rozwoju, Organizacji i Funkcjonowania, Toruń, 2013.

[17] LARSSON, A. O., Online, all the Time? A Quantitative Assessment of the Permanent Campaign on Facebook, in: New Media and Society, 18(2), 274-292, 2016.

[18] LESZCZUK-FIEDZIUKIEWICZ, A., Internet jako Narzędzie Kreowania Wizerunku Polityka, in: Nowe Media. Czasopismo Naukowe, 2, 31-54, 2011.

[19] NOWINA-KONOPKA, M., Rola Internetu w Rozwoju Demokracji w Polsce, Kraków – Nowy Sącz, 2008.

[20] PIONTEK, D., Komunikowanie Polityczne i Kultura Popularna. Tabloidyzacja Informacji o Polityce, Poznań, 2011.

[21] SCAMMEL, M., The Media and Media Management, in: A. Seldon (ed.) The Blair Effect, London, 509-533, 2001.

[22] SMITH, J. F., Obama Adopting Permanent Campaign Strategy, Boston, 2009.

[23] SOBACI, M. Z., ERYIGIT, K. Y., and HATIPOGLU, I., The Net Effect of Social Media on Election Results: The Case of Twitter in 2014 Turkish Local Elections, in: Social Media and Local Governments, 265-279, 2009.

[24] STRANDBERG, K., Online Campaigning: An Opening for the Outsiders? An Analysis of Finnish Parliamentary Candidates' Websites in the 2003 Election Campaign, in: New Media and Society, 11(5), 835-854, 2009.

[25] VERGEER, M. and HERMANS, L., Campaigning on Twitter: Microblogging and Online Social Networking as Campaign Tools in the 2010 General Elections in the Netherlands, in: Journal of Computer-Mediated Communication, 2013.

[26] WARD, S. J., GIBSON, R. K., LUSOLI, W., Online Participation and Mobilization in Britain: Hype, Hope and Reality, in: Parliament Affairs, 56(4), 652-668, 2003.

[27] WEINER, M. D., The Party's Still on: American Political Parties from 1950 to 2005, in: R. A. Harris, D. J. Tichenor (eds) A History of the U.S. Political System, Santa Barbara, 22-40, 2010.

[28] ZARĘBA, A., Permanent Campaign in Poland – Causes, Elements, Importance, in: Political Preferences 13, 97-113, 2016.

EFFECTS OF DIGITALIZATION ON THE LABOR MARKET IN BADEN-WUERTTEMBERG

Oliver Sievering[1]

DOI: 10.24989/ocg.v331.39

Abstract

The technological change is constantly progressing. Digitalization opens up great opportunities for a higher quality of life. It enables more efficient business models and it also has a significant impact on the labor market. More and more tasks, which could be done only by humans so far, will be taken over by computers or robots in the future. It is controversial whether digitalization will lead to a higher unemployment or to a growth in employment because digitalization also creates new kind of jobs. While the impact on labor markets can not be clearly predicted, the fear of digitalization is huge. Many employees in Germany have jobs with a high potential of substitutability. The proportion of employees affected by severe effects of digitalization is estimated to range from 8.1% to 20.4% - depending on the federal-state. In Baden-Wuerttemberg, a very high substitution potential is assumed. Will unemployment significantly rise in the southwest part of Germany?

1. Introduction

With the use of computers and automation by robots since the 1970s and 1980s, Industry 3.0 began. Today, industrial development with the keyword “Industry 4.0” enters its fourth, fundamental transformation in which comprehensive digitalization of production processes and business models play a key role. The term stands for the interactive networking of analog production with the digital world. This transformation includes elements such as big data, autonomous systems, cloud computing, social media, mobile and self-learning systems. Production and logistics processes within companies and between companies can be interlinked intelligently in order to make production even more efficient and flexible. A largely self-organized production cycle becomes possible. The term "Industry 4.0” originates from a project of the high-tech strategy developed by the German government. The meaning of “Industry 4.0” as a revolution is often criticized in view of the fact that technological innovation is a more or less continuous process. However, digitalization not only affects the industry, but almost all sectors of the economy, including the service sector and the public sector. In healthcare for example, innovative digital telemedicine applications could provide new ways to increase the effectiveness and efficiency of service delivery, improve patient care and increase transparency of services and value-added processes. The digitalization of work processes is changing the economy profoundly. Many people perceive digitalization as a threat and not as an opportunity. In the media and in public debates, threat scenarios often attract more attention than scenarios outlining potentialities. The fear of an imminent wave of technologically induced unemployment is one of the dominant political and policy topics of our time. Many employees could be replaced by new and smarter machines and computers; tasks formerly carried out only by humans.

[1] Hochschule für Öffentliche Verwaltung und Finanzen, Ludwigsburg.

With a view to the future development of the labor market, central questions are: How will digitalization affect employment? Will jobs be replaced and if so, who will be affected particularly? Formerly, the answer was clear: Jobs with low wages and especially jobs for low-skilled worker will be replaced. In the current discussion, the thesis is present that more and more activities in the mid-level of qualification, especially those with a high degree of routine, could automated. In Germany, there is some evidence that the importance of routine skills with a medium qualification will decline.

It is controversial whether the progressive digitalization of the economy leads to a reduction in employment or to an employment growth. It is quite possible that digitalization is even leading to employment growth: the computer-controlled machines and devices must be developed and built. Qualified staff is needed to program the associated software. The machines and equipment need to be controlled and maintained. However, qualified employees who can handle the new technology will have to be trained. This in turn requires trainers as well as software specialists who develop tutorials or impart new technologies. The impact of digitalization on labor markets can`t clearly be predicted.

2. Studies

Current studies intensely discuss the question of whether and to what extent unemployment is to be feared in consequence of digitalization. The debate about the impact on the labor market and employment evolves around two major perspectives: a pessimistic and an optimistic one. Optimists believe in significant employment growth. They do expect an increase of employment in total. Pessimists however believe that current technological developments will provoke massive job losses. Some studies and popular science articles have even fueled a debate about an "end of work". They focus on the automation potential of digitalization: Intelligent machines and algorithms would replace many employees in the middle and long term. But already the invention of the loom, the steam engine or robots in the 1970s have repeatedly led to similar predictions.

An authoritative input to the effects of robotics and artificial intelligence on the working environment came from Frey and Osborne of the University of Oxford in the year 2013. They examined the potential of digitalization/automatization in the USA. Based on an expert survey, they have estimated the automation potential for 702 occupations. They estimate that 47% of American workers do jobs which could be replaced by computers and algorithms over the next 10 to 20 years. [7] Based on a specific task approach, a job has a high risk of automation if it is composed of more than 70% routine activities. Frey and Osborne point out that low-skilled and low-paid employees are affected mostly by digitalization. In particular, industrial occupations like mechatronics (81%), toolmakers (84%) or assembly worker (97%) have a high probability of automation. On the contrary, jobs requiring creative intelligence (e. g, art, creative problem solving) and tasks requiring social intelligence (e.g. negotiate, convince) tend to have a low probability of automation. According to the authors, workers in the transport and logistics sector are also particularly at risk. In the medium term, self-driving cars or drones could take over a large part of the goods delivery or postal delivery. In the service sector, the fear of substantial rationalization effects is significant too.

This study, especially its prognosis, was criticized. The statement that 47% of the jobs in the USA are at risk of automation implies that everything that could be automated theoretically will be automated in practice. The results are based on a great extent on subjective assessments of robotic and digitalization experts. These experts tend to overestimate the potential impact and practical relevance of new technologies. Furthermore, technical automation potentials are not necessarily

implemented in a timely manner. Another major aspect is that the focus of the discussion is on the threat potential of existing employment relationships. The authors explicitly ignore the emergence of new fields and new jobs - and thus possible positive employment effects. In addition, in determining the technical potential, social, legal and ethical hurdles in the introduction of new technologies aren`t taken into account. Consequently it could be argued, that the real automation potential is probably (much) lower. At the same time it needs to be positively noticed, that the authors vividly illustrate how automation technologies continue to advance into areas of activity previously reserved only for humans. In doing so, the authors address an under-researched topic whose significance is likely to increase in importance in the future due to rapid technological development. [1]

Other studies have transferred the findings to Germany. Based on a detailed breakdown of jobs in Germany, Brezki and Burk transferred Frey`s and Osborne`s results to the German labor market and calculated how many jobs in Germany are endangered. In this study, 30.9 million socially insured and marginally employed persons are considered. 18.3 million among them (59%) are threatened by progressive technologization/digitalization in Germany. (See table 1) [1]

	Employees subject to social security contributions and marginally employed	Endangered jobs due to digitalization	likelihood
Investigated occupations	30,870,000	18.300,000	59%
Office employees	3,500,000	3.000,000	86%
Elementary occupations	3,800,000	3.260,000	85%
Machine operators, assemblers	4,640,000	3.210,000	69%
Service and sales professions	4,570,000	3.120,000	68%
Craftmens	4,100,000	2.580,000	63%
Academic professions	3,990,000	471,000	12%
Executive persons	1,380,000	157,000	11%

Table 1: Endangered jobs due to digitalization [1]

Administrative employees such as secretaries or clerks are subject to the highest risk (86%), followed by ancillary workers (85%). Mechanics, drivers and operators of machines are also particularly affected (69%). Looking at the individual occupations, the following jobs could be regarded as having a high potential of rationalization via digitalization: Office and secretarial staff (1.9 million), employees in postal and delivery auxiliaries and warehousing (1.5 million), salesmen (1.2 million), cleaning assistants (1.1 million) and catering service workers (661,570). The use of drones, automated processes in warehouses and transport could replace up to 1.5 million jobs. Altogether, the named professions alone make up 6.3 million jobs at risk. Digitalization will also affect particularly public administration, the manufacturing sector and machine controlling professions. Executives, as well as academics in scientific and creative professions are seen as having a minor likelihood of being replaced. [3]. Overall, there will be a shift towards IT activities in almost all professions.

Bonin et al. initially draw the conclusion that 42% of jobs in Germany are endangered - following Frey's and Osborne's approach. [1] But they change the approach to estimate the impact of digitalization on the labor market. They argue in a narrow sense, that only concrete activities will be automated not however entire jobs. For this purpose, the automation probabilities are transferred on the basis of the job structure at the workplace. Taking this method into account only 12% of employees in Germany and 9% of employees in the US are endangered by digitalization in the next 10 to 20 years.

The IAB (Institut für Arbeitsmarkt und Berufsforschung) estimates that in 2015 about 15%, approximately 4.5 million, of the employees (subject to social insurance contributions) in Germany have a job with a high potential of substitution. [5] These two studies (Bonin et al. and IAB) thus predict moderate rationalization effects.

It also must be taken into account that growth effects might be caused by digitalization. Technical progress can create new tasks and jobs. Several long-term forecasts on the development of the labor market have already been prepared on behalf of the BMAS (Bundesministerium für Arbeit und Soziales; Federal Ministry of Labor and Social Affairs). The study by Vogler-Ludwig / Düll / Kriechel on behalf of the Federal Ministry of Labor and Social Affairs comes up with a positive result. Its key finding is that in a baseline scenario, the workforce in 2030 will be at about the same level as in 2014, while the scenario of accelerated digitalization, due to productivity effects, may even have a significant positive impact on growth and employment. This would result in an additional loss of total 750,000 jobs in 27 sectors (e.g. retail, paper and printing, public administration), but also generate one million additional jobs in 13 other sectors (e.g. IT services, research and development). On balance, employment could rise by approximately a quarter of a million people by 2030. [13]

The long-term effects on the labor market were also estimated in the context of the BIBB-IAB qualification and occupational projections. According to this study, the expected net labor market effects are to be neglected. By the year 2025, a decline of only around 60,000 workers is expected. [14]

Further studies draw similar results. They do not predict significant employment losses but a significant change in labor structure. The „Sachverständigenrat zur Begutachtung der gesamtwirtschaftlichen Entwicklung“ in Germany draws the same conclusion. Although digitalization will change the world of work in the middle and long term, there are no negative macroeconomic effects to date. [10] All studies assume that machines/computer are likely to take over primarily more routine work.

Furthermore it is assumed that automation/digitalization will replace not only low-skilled activities but in particular medium-skilled activities with a high degree of routine work. This could lead to an employment polarization, a relative increase of low-skilled and high-skilled employment. The studies also indicate that activities requiring a high level of emotional and social skills, as well as those requiring a willingness to innovate and the ability to think analytically, will be the least affected by digitalization. Cognitive activities will only partially replaceable. These include, for example, managerial occupations, social, medical and health professions. Among the experts there is slightly potential for substitutable tasks too. On the other hand, digitalization affect particularly the public administration, the manufacturing sector and machine controlling professions. [6]

3. Regional impacts

The IAB, estimating a rationalization potential of 15 % (approximately 4.5 million jobs) in Germany due to digitalization (see chapter 2), has also examined its regional impact. Accordingly, the proportion of activities that could be done by computers and computer-controlled machines varies considerably between occupations. Therefore, the occupational and thus the economical structure largely determines the possible labor market effects of digitalization in each federal state.

The potential of substitution varies between 8.1% and 20.4% among federal states. The higher the importance of the manufacturing sector in a federal state, the higher the proportion of employees with a high potential of substitution tends to be and vice versa. This is in particular discernible in Berlin and Hamburg, where the proportion of employees in the manufacturing sector is only about 11% and 15% (see table 2). In these cities, many employees work in occupations of corporate management and organization or in business-related services, which have a significantly lower potential of substitution. In Berlin, there is an above-average number of employees working in the social and cultural sector - occupations with a low potential of substitution. In federal city-states, the service sector is generally much more pronounced. As a result, Berlin is least affected. It has the lowest share of employees in the manufacturing sector (11.5%) and so it has the lowest potential of substitution (8.1%). [4]

Significantly above average is the proportion of the manufacturing sector in Baden-Wuerttemberg and in Saarland. The share of the manufacturing sector (measured by the gross value added) is more than 30% respectively; in Saarland 31.3% and in Baden-Wuerttemberg 35.4% (see table 2). A hint: The manufacturing industry in Germany plays a much more important role than in other developed countries: Compared with other economies such as France (19.5 %), the United Kingdom (20.2 %) or the United States (20.7 %), the share of the German manufacturing sector is significantly higher in terms of gross domestic product (and also measured in gross value added). Baden-Wuerttemberg has the highest proportion of employees subject to social insurance contributions in the manufacturing sector in Germany. A particularly large number of employees are working in mechanical engineering and in the automotive industry. Therefore, the potential of substitution in Baden-Wuerttemberg is relatively high. In Baden-Wuerttemberg, this applies to around 753,400 employment relationships that corresponds to a potential substitution of around 17.4% of total employees. [4] However, the correlation between the proportion of the manufacturing sector (measured by gross value added) and the substitution potential is not perfect but the correlation coefficient is very high: 0.89.

Federal states	Unemployment rate (2017)	Proportion of manufacturing sector (measured by gross value added)	Potential of substitution
Baden-Wuerttemberg	3.5	35.4	17.4
Bavaria	3.2	29.3	15.4
Berlin	9.0	11.5	8.1
Brandenburg	7.0	20.3	12.1
Bremen	10.2	25.1	13.3
Hamburg	6.8	15.0	9.3
Hesse	5.0	20.3	13.1
Mecklenburg-Hither Pomerania	8.6	15.3	10.8
Lower Saxony	5.8	25.0	15.2
North Rhine-Westphalia	7.4	23.6	15.6
Rhineland-Palatinate	4.8	29.3	15.3
Saarland	6.7	31.3	20.4
Saxony	6.7	24.7	15.9
Saxony-Anhalt	8.4	25.7	14.6
Schleswig-Holstein	6.0	18.5	12.0
Thuringia	6.1	27.0	18.8
Germany	5.7	25.7	15.0

Table 2: Unemployment rates, proportion of manufacturing sector, potential of substitution

Within Baden-Wuerttemberg too, there are considerable regional differences. The differences at county level can be explained to a large extent - as well as the level of the federal-states - on the

basis of the varying importance of the manufacturing sector. In cities like Heidelberg and Freiburg, low levels can be explained by an above-average proportion of employees in the social and cultural service sector and in the medical health sector, for whom the potential of substitutability is particularly low. In rural areas like Tuttlingen, Rottweil and the Enzkreis, however, service occupations with low substitutability potential play a subordinate role, while manufacturing and manufacturing occupations with a high proportion of manual routine activities are considerably overrepresented. (see table 3) The correlation between substitution potential and number of persons working in the manufacturing sector is not perfect, but similar to the federal-states, also significant. In addition, some regional characteristics must be considered. [10]

	Potential of substitution
Baden-Wuerttemberg	17.1
Heidelberg	9.1
Stuttgart	9.6
Freiburg	9.7
Karlsruhe	10.1
Heilbronn	14.3
Ludwigsburg	15.1
Rottweil	28.6
Enzkreis	28.8
Tuttlingen	32.1

Table 3: Proportion of substitutional potential in selected districts in Baden-Württemberg [10]

4. Current labor market situation in Germany

The German economy continues its moderate upswing in 2017 and 2018. Important reasons of economic growth are the domestic consumption and the export, which support a positive development on the labor market. The number of employed persons is growing furthermore. In 2017, it has reached the highest level since reunification in 1991. (see table 4) [11]

Year	Working population (in 1,000)	Volume of work (millions hours)
1991	38,790	60,261
1995	37,958	57,999
1999	39,031	57,716
2005	39,326	55,500
2009	40,892	56,133
2013	42,328	57,657
2016	43,486	59,281

Table 4: Working population, volume of work [11]

The number of the working population increased from 38.8 million in the year 1991 to 43.5 million in 2016. This corresponds to an increase of more than 12%. However, the increase in the labor force did not go hand in hand with an increase in the volume of work. The annual number of hours worked by the employed fell from 60 billion in 1991 to 55.5 billion in 2005. That corresponds to a minus of almost 8%. One major reason for this reduction was the reunification. In the 1990s, it led to a significant job loss in Germany, especially in the eastern part, but since 2005, annual working hours increased, reaching an hourly volume of over 59 billion hours in 2016. Although digitalization has progressed for years, the "work did not go out" - on the contrary: more workers and a higher workload are recorded in Germany.

The rate of unemployment – in comparison to other European states - is very low in Germany, especially in Baden-Wuerttemberg (3.5%) and Bavaria (3.2%). In some regions of these federal-states, especially in the south, it is less than 2.5%. The overall job vacancy in the third quarter of 2017 was 1.1 million jobs in Germany. [9] The rising number of job vacancies in the last years indicates that it is becoming more and more difficult for companies to find suitable employees. Although it can not be said there is a widespread shortage of skilled workers, bottlenecks in some technical jobs, such as the information and communication sector, construction professions as well as some social, health and care professions are evident.

In Baden-Wuerttemberg, the bottleneck of skilled workers is more noticeable than in most other federal states. Here in addition to the nationwide bottlenecks as mentioned above, there are bottlenecks in numerous industrial and craft trades, but also in manufacturing. There is also a bottleneck in the vehicle, aerospace and logistic sector, in civil engineering and building construction. In the next years, the shortage of skilled workers will increase significantly due to the demographic change. (see chapter 5). Furthermore the labor market experts expects a significant growing labor demand in business-related services, in the building sector, information and communication sector, social services especially health care and elderly care, scientific and in the field of polymer processing and electrical engineering due to the moderate economic growth. [2] The shortage of skilled workers is getting bigger.

5. Demographic change and digitalization

Demographic change will aggravate this trend in the next years. The working-age population will be severely affected by shrinkage and aging despite the influx of many (young) migrants. The main reason for this is a very low birth rate. The fertility rate is only 1.4 - 1.5, making it one of the lowest in Europe. In recent years, significantly more people retired than young people moved up from the school system (or from universities) to the labor market. This demographic effect amounted to approximately 300,000 persons only in 2016 - tendency to rise.

This trend affects the number of working population, aged from 20 to 64 years. In 2013, 49.2 million people belonged to this age group. Their number will decrease significantly after 2020. The decline in potential labor force – if the baby-boomers (born in the 1960s) retire – will accelerate in the next decade. In 2030, the number will be approximately 44 - 45 million. In 2060, approximately 38 million people will be in the working age (- 23%) if the migration balance gradually falls from around 500,000 in 2014 to 200,000 by 2021 and then remains constant (Option 2 "Continuity of increased immigration"). If immigration decline to 100,000 people every year by 2021 and then remains constant (option 1 "Continuity of weaker immigration"), there will be an even more decreased potential labor force in 2060: 34 million or - 30% compared to 2013. [6]

Population in Germany	year	mio.
population overall	2013	80.8 mio.
20-64 years (age)	2013	49.2 mio.
Development with weaker immigration:		
Population overall	2060	67.6 mio.
20-64 (age)	2060	34.3 mio.
Development with stronger immigration:		
Population overall	2060	73.1 mio.
20-64 (age)	2060	37.9 mio.

Table 5: Demografic change [6]

Assumption:
Birth rate 1.5 children per woman, life expectancy at birth 2060 for boys 84.7 / girl 88.6 years, external migration balance decreases from 750 000 in 2016 to 200 000 in 2021, then constant (G1-L1-W2015)
Birth rate 1.4 children per woman, life expectancy at birth 2060 for boys 84.8 / girl 88.8 years, external migration balance decreases from 500 000 in 2014 to 200 000 in 2021, then constant (G1-L1-W2)

Accordingly, the demographic change has a dominant effect. The number of working people in Germany is falling faster than the total population. The bottleneck of skilled worker is getting bigger in coming years. The potential labor shortage will cover a wide range of jobs, specialists and occupations. The biggest bottlenecks occur in the service sector (especially health and care) also in research and development. Overall, there is a potential labor shortage of 3.9 million workers by 2040. For the service sector, there is predicted a potential gap of 2.8 million workers nationwide by 2040. With a potential staff shortage of around 1.5 million in 2040, most workers in the public and other service providers, education and health will be missing, thereof one million people in the health and social services. [2] From the year 2025 onwards, when the baby boomers are going to retire, the situation will be worsening in more and more occupations. Digitalization can therefore be an opportunity to counteract the bottleneck of skilled workers in Germany. But the lack of skilled workers will be significant in business-related services, social and health professions. In these sectors, productivity progress is relatively low and the potential for substitution due to digitalization is relatively low too, the shortage of skilled workers is unlikely to be remedied. Digitalization can solve this problem only partially. Due to the demographic change, the bottleneck of many jobs will get worse. This is especially true in the federal states, having already low unemployment rates, as in the case for example in Baden-Wuerttemberg.

6. Conclusion

In the discussion on the consequences of digitalization, fears of a massive loss of jobs conflict with the hope for innovation and employment gains. Most studies point up that the fear of a massive job loss in the course of further digitalization is currently unfounded, but there are also studies that predict significant rationalization potential in many occupations. Whether the effects of technological change on the production process and society will have a revolutionary character will eventually only be answered in retrospective.

Even if these studies have different approaches and time horizons, the studies indicate a certain order of magnitude. The potential of substitution about one-seventh to one-eighth of the workforce, is quite significant, though far away from the 47% of Frey/Osborne's original study and it does not mean the "end of work". In recent years, both the number of employed persons and the number of working hours have increased considerably in Germany, despite ongoing digitalization. However, the progressive digitalization can at least counteract partially the shortage of skilled workers caused - in particular - by demographic change.

The progressive digitalization of the work environment poses somewhat bigger challenges for Baden-Wuerttemberg than most other federal states: the share of employees subject to social security contributions who work in a profession with high substitutability potential is clearly above average, compared to other federal-states. The higher number can be explained largely by the specific economic structure in Baden-Wuerttemberg. The manufacturing sector and thus also the production occupations are of great importance here, but these occupations have at the same time a high potential of substitutability.

In Baden-Wuerttemberg unemployment is currently very low and will decline in the next years furthermore. The bottleneck of skilled worker that currently exists in some sectors will intensify - despite ongoing digitalization. Digitalization will only partly eliminate skills shortages, but rather exacerbate in some areas. New employment opportunities will arise in many sectors where bottlenecks exist, for example in the IT professions. In the social and health professions, where there is currently an acute bottleneck of skilled workers too, the substitution potential of digitalization is low. The author does not see "an end of work" (at least until the year 2030), especially in Baden-Wuerttemberg - on the contrary - in many professions there will be a wider shortage of skilled workers.

7. References

[1] BONIN et. al., Übertragung der Studie von Frey/Osborne (2013) auf Deutschland, 2015, ZEW ftp://ftp.zew.de/pub/zew-docs/gutachten/Kurzexpertise_BMAS_ZEW2015.pdf

[2] BRÄNDLE, Tobias; MORLOCK, Miriam; Digitalisierung in Baden-Württemberg; Stand der Digitalisierung in den Betrieben und potenzielle Implikationen; IAW- Kurzbericht 1/2017; Institut für angewandt Wirtschaftsforschung. http://www.iaw.edu/tl_files/dokumente/iaw_kurzbericht_2017_01.pdf

[3] BRZESKI, Carsten; BURK, Inga (2015): Die Roboter kommen - Folgen der Automatisierung für den deutschen Arbeitsmarkt; Economic Research 2015; https://www.ing-diba.de/pdf/ueber-uns/presse/publikationen/ing-diba-economic-research-die-roboter-kommen.pdf.

[4] BUCH, Tanja; DENGLER, Katharina und MATTHES, Britta; Relevanz der Digitalisierung für die Bundesländer Saarland, Thüringen und Baden-Württemberg haben den größten Anpassungsbedarf; IAB-Forschungsbericht, 14/2016. http://doku.iab.de/kurzber/2016/kb1416.pdf

[5] DENGLER, Katharina; MATTHES, Britta (2015): Folgen der Digitalisierung für die Arbeitswelt. Substituierbar-keitspotenziale von Berufen in Deutschland. IAB-Forschungsbericht Nr. 11, Nürnberg. http://doku.iab.de/forschungsbericht/2015/fb1115.pdf

[6] destatis, Statistisches Bundesamt; Bevölkerung Deutschlands bis 2060. https://www.destatis.de/DE/PresseService/Presse/Pressekonferenzen/2015/bevoelkerung/Pressebroschuere_Bevoelk2060.pdf?__blob=publicationFile

[7] FREY, C. B., OSBORNE, M. A. (2013), The future of employment: how susceptible are jobs to computerisation?,Oxford Martin School Working Papers, September; http://www.futuretech.ox.ac.uk/sites/futuretech.ox.ac.uk/files/The_Future_of_Employment_OMS_Working_Paper_0.pdf.

[8] HAFENRICHTER, Julia et. al. Digitalisierung der Arbeitswelt, Folgen für den Arbeitsmarkt in Baden-Württemberg IAB Baden-Württemberg in der Regionaldirektion Baden-Württemberg 3/2016 S. 24 ff. http://doku.iab.de/regional/BW/2016/regional_bw_0316.pdf

[9] IAB; Presseinformation des Instituts für Arbeitsmarkt- und Berufsforschung vom 8.8.2017. http://www.iab.de/de/informationsservice/presse/presseinformationen/os1702.aspx

[10] Sachverständigenrat zur Begutachtung der gesamtwirtschaftlichen Situation, Jahresgutachten 201772018, 2017. pp. 35. https://www.sachverstaendigenrat-wirtschaft.de/fileadmin/dateiablage/gutachten/jg201718/jg2017_04_wipo.pdf

[11] Sozialpolitik aktuell; Jahresarbeitsvolumen und Zahl der Erwerbstätigen http://www.sozialpolitik-aktuell.de/tl_files/sozialpolitikaktuell/_Politikfelder/Arbeitsmarkt/Datensammlung/PDF-Dateien/abbIV4.pdf

[12] Statista: Arbeitslosenquote Deutschland https://de.statista.com/statistik/daten/studie/1224/umfrage/arbeitslosenquote-in-deutschland-seit-1995/

[13] VOGLER-LUDWIG, Kurt; DÜLL, Nikola; KRIECHE, Ben; Arbeitsmarkt 2030 – Wirtschaft und Arbeitsmarkt im digitalen Zeitalter Prognose 2016; Im Auftrag des Bundesministeriums für Arbeit und Soziales; http://www.economix.org/assets/content/Arbeitsmarkt%202030/Vogler-Ludwig%20et%20al%202016%20Arbeitsmarkt%202030%20-%20Wirtschaft%20und%20Arbeitsmarkt%20im%20digitalen%20Zeitalter.pdf

[14] WOLTER, Marc Ingo et al. IAB-Forschungsbericht 8/2015 Industrie 4.0 und die Folgen für Arbeitsmarkt und Wirtschaft Szenario-Rechnungen im Rahmen der BIBB-IAB-Qualifikations- und Berufsfeldprojektionen. IAB-Forschungsbericht 8/2015. http://doku.iab.de/forschungsbericht/2015/fb0815.pdf

Emergency Communications and Alerting Systems for Fire Brigades in Baden-Württemberg – Much Room for Improvement?

Eva Gräßle[1] and Robert Müller-Török[2]

DOI: 10.24989/ocg.v331.40

Abstract
Most of the fire brigades in Baden-Württemberg are volunteer forces, hence creating the need for readily available and reliable alerting and communication systems for these forces as well. Digital Pagers are the standard means of alerting but, due to their limited reliability, alternative and complementary methods like Apps, SMS, etc. are also used by these volunteer forces. Regarding communication at the scene, the transition from open analogue to encrypted digital radio systems has been on its way for nearly 20 years. As of today, new technology is available for police forces whilst fire brigades still have to use analogue systems. This contribution analyses the situation, past and present, planning and attempts at improvement.

1. Introduction

In recent years a significant increase in large scale emergencies, caused by terrorism and crime, was observed in "The West", namely in the USA and UK, France, Belgium and also in Germany. The violence during the G20 summit in Hamburg 2017 [6, 7, 8] and the deadly attack by an Islamic terrorist, with a truck, on the Christmas Market on Breitscheidplatz in Berlin [9, 10], were not simply police issues but they also called for the fire brigades' involvement. Terrorist attacks in the past included trucks (Nice and Berlin), cars (London) and, never to be forgotten, by airplanes in the 9/11 attack against the Pentagon and the Twin Towers in New York. Police assisted in the latter, but it was mainly an operation by the Fire Department of New York (FDNY). So the issue of alerting and communicating systems for fire brigades becomes more vital, especially when we consider combined attacks against airports, refineries or chemical plants, all of which can occur in a quite remote and peaceful land like Baden-Württemberg[3].

The municipalities – in Baden-Württemberg, 1.101 entities plus 35 counties or "Landkreise", have the legal obligation to organize fire brigades, each as "a capable fire brigade according to the local requirements" (§ 3 (1) FwG BW, our translation), which leaves a lot of room for interpretation. The municipalities must organize it on their own, i.e. they are not bound by any orders from a central authority such as the Federal State Ministry of the Interior (see § 2 (2) FwG BW). According to the interpretation of the Federal State Association of Fire Brigades, the term "capable" means

[1] Civil Servant, City of Schwieberdingen, Schloßhof 1, D-71701 Schwieberdingen. The views expressed in this paper are the private opinion of the author.
[2] Professor, University of Public Administration and Finance Ludwigsburg, Reuteallee 36, 71634 Ludwigsburg, Germany. Email: mueller-toeroek@hs-ludwigsburg.de
[3] The Kelley Barracks, HQ of the United States Africa Command AFRICOM are only 5 kilometers away from Stuttgart International Airport; the world's biggest chemical plant, BASF Ludwigshafen is situated in the twin cities of Ludwigshafen-Mannheim, the latter belonging to Baden-Württemberg and the largest refinery of Germany, MiRo is situated in the Baden-Württemberg town of Karlsruhe [2].

- Response Time, i.e. the time in which a dispatched fire engine arrives on the scene
- Firefighters, i.e. sufficient staff available on the scene
- Equipment available on the scene should be appropriate [3].

This leaves much room for discussions between councilors, civil servants, mayors and of course firefighters, about the necessary equipment, the topic on which we focus in this paper. In the following sections, we describe the state of alerting and communicating systems and finally ask if they appear to be sufficient for likely events such as major terrorist attacks or other large scale incidents.

In Germany the Ambulance Service is mostly provided by the Fire Brigades[4], only a minor share of the service being provided by the German and Bavarian Red Cross and private entities. The emergency number 112 is both for fire brigade related and medical emergencies and is mostly operated by the local fire brigade command.

2. Some core figures on the fire brigades of Baden-Württemberg

Fire brigades in Baden-Württemberg belong to the so called "Authorities and Organizations tasked with Security" and are organized in voluntary fire brigades and in professional brigades consisting of regularly employed firefighters. A professional fire brigade is mandatory for municipalities with more than 100,000 inhabitants – a criterion not met by many, hence there being only some 2,100 professional firefighters serving in the Federal State [4]. In addition, some companies are required to run their own fire brigades[5], e.g. the above mentioned BASF for their chemical plant.

In the whole Federal State a total of some 116,676 firefighters served, as per 2016 [5], which means that roughly two percent of the firefighters are professionals, the vast majority being volunteers.

3. Alerting Systems

To provide alerting systems is the task of the counties and the Federal State does not provide such systems (see § 4 (3) FwG BW). The current alerting system is the Digital Pager. Quite handy, approximately the size of a cigarette box, it is equipped with a small display and a small keyboard. The system in Baden-Württemberg is based on the 2m frequency band which is reserved for alarm warnings only, so that the 4m band can be used for communications on the scene. In recent years additional systems were introduced but they only supplemented the Digital Pager which is the sole official means of alerting/warning/alarming.

The costs for such additional systems cannot be borne by the counties, their legal obligation to provide an alerting system being fulfilled by the Digital Pagers. Such systems are mainly SMS or App-based. These costs can be borne by the respective municipality but some of them refuse, citing the Digital Pagers.

[4] Namely in larger cities like Munich, Hamburg, Berlin, Essen etc. In rural areas the Red Cross and other organizations operate a larger share of the ambulance services.
[5] See § 19 (1) FwG (BW).

Additional systems have a positive effect if the main alerting system is not available. Some counties and municipalities have legal doubts, especially when the alarm concerns not a fire brigade issue but an ambulance issue. In the latter case sensitive personal data is transferred via a non-secure network, such as the internet or the mobile phone network, such that the dispatchers in the county of Ludwigsburg refrained from using these additional alerting systems (see [1], p. 16). Note that the mobile phone networks in Germany use AES in versions of a grade lower than A5/3. The biggest German mobile phone network provider, Deutsche Telekom AG, announced the introduction of A5/3 in late 2013 [11]. Even in 2018 we cannot be sure that all providers will use an advanced encryption standard, which cannot be hacked into in real time, as was the case with the outdated A5/1 standard [18].

4. Communication Systems

Open analogue radio is unfortunately still the standard when it comes to communications on the scene. The conference of the Ministers of the Interior of Germany announced the introduction of encrypted digital radio systems in 1996, but the replacement is far away from being implemented (see [1], p. 25). A major issue with the analogue radio is that any communication can be intercepted easily – given a scenario of a planned terrorist attack, like that in Mumbai on November 26th, 2008, the terrorists will have the necessary equipment to intercept the communications of the emergency services [12].

After several political acts since 1996 finally, in 2006, a Federal Agency was founded with the task of introducing a standardized, encrypted digital radio system for all the relevant organizations in Germany – a task not yet completed. As of 2017 the police forces used digital radio, but not the "non-armed" organizations like Fire Brigades, Red Cross and the THW[6].

This leads to another major shortcoming of the current regime: e.g. if Federal State Police, local Fire Brigade, Red Cross and Commandos from the Federal Police work together on one scene, how shall they communicate? They have no common system and there is no interoperability between digital and analogue radio. The lucky Fire Brigades, whose counties and municipalities financed their transition to encrypted digital radio, must also bring their old analogue radios with them in order to be able to communicate with the less fortunate forces on the scene.

Other countries, despite being at the same industrial and economic level as Germany, have similar issues. Japan has transformed its respective fire prevention organizations within the last years; according to industry sources [see 19, p. 53]. The advantages of digitized wireless communications are quite obvious [see 19, pp. 55].

5. Availability of the Alarm and Communication Systems

Scenarios like Mumbai 2008, where the siege of the Taj Mahal Hotel lasted for three days, or Paris Bataclan, can easily last for many hours so the question arises on the availability of the communication systems of the emergency forces. Imagine that telephones and the power grid are down, at least for a while and look what happens:

[6] Technisches Hilfswerk, a German Federal Agency in charge of Disaster Relief Operations nationwide and also worldwide.

5.1. Availability of the Digital Pagers

The dispatcher system becomes redundant and decentralized; such availability can be taken for granted (see [1], p. 41).

5.2. Availability of additional alerting systems, SMS or app. based

Both, SMS and App are heavily dependent upon the availability of the mobile phone network and the internet, e.g. as shown on http://allestörungen.de/, a website collating all errors and instances of non-availability of German Telecommunication Providers. Local non-availability is quite normal, both of mobile phone network and internet services.

5.3. Availability of the open analogue radio

Given power supply, which is also provided from fire engines, the availability of this is very high.

5.4. Availability of the encrypted digital radio

A formal inquiry to the Federal Government by a Member of Parliament in 2016 showed a very disappointing result: A failure of the national power grid can be compensated for, by a decentralized power supply for only two hours [13]. This means that after just two hours, the encrypted digital radio used by police forces is no longer available. Further evidence shows that this is not the only shortcoming of the digital radio systems operated:

- On July 22nd, 2016 a juvenile went on a killing spree in Munich. Digital Radio of the Bavarian Police forces was unavailable for minutes, forcing the police to resort to the use of private mobile phones [14]
- On New Year's Eve in Cologne the Digital Radio of the Cologne Police was unavailable [15]
- During the recent terrorist attacks in Brussels, Belgian Police had to resort to WhatsApp (sic!) because their digital radio did not work [16]

Without discussing this alarming issue further, it is worth mentioning that the Senate of the Federal State of Berlin, the capital of Germany, voted in 2017 to buy some 16,000 regular mobile phones for the Berlin Police - simply because the Digital Radio available is not reliable [17].

6. Resume

Modern Alerting and Communication Systems can definitely bring added value to both the fire brigades and the society served. Due to the massive trend towards digitalization, current alerting systems must be changed, bearing in mind that new technologies are not per se 100 percent reliable and can be interrupted with little effort. Digital pagers will likely remain the most reliable alerting method. The big issue seems to be the analogue radio systems which still operate, the transition to encrypted digital radio systems is still on its way, even after a decade and its completion cannot be predicted with any certainty.

A major security issue is the limited availability of emergency power supply for the digital radio systems – two hours is definitely not sufficient when compared to the current threat scenarios, which include daylong stand-offs and operations lasting far more than two hours.

7. References

[1] Moderne Alarmierungs- und Kommunikationssysteme der BOS - Eine kritische Betrachtung am Beispiel der Feuerwehr. Bachelor Thesis, University of Public Administration and Finance Ludwigsburg by Eva Gräßle, 2017.

[2] "Der Karlsruher Ölriese - Deutschlands größte Raffinerie", by Robin Szuttor, in Stuttgarter Zeitung, 4.12.2012.

[3] Landesfeuerwehrverband Baden-Württemberg e.V.: Hinweise zur Leistungsfähigkeit der Feuerwehr, Seite 3; URL: http://www.fwvbw.de/fileadmin/Downloads/allgemein/Hinweise_zur_Leistungsf%C3%A4higkeit_einer_Feuerwehr.pdf (as per 25.08.2017)

[4] Landesfeuerwehrverband Baden-Württemberg e.V.: Feuerwehren, Berufsfeuerwehr; URL: http://www.fwvbw.de/berufsfeuerwehren,92.html (as per 28.07.2017).

[5] Landesfeuerwehrverband Baden-Württemberg e.V.: Zusammenfassung der Jahresstatistik 2016; URL: http://www.fwvbw.de/fileadmin/Downloads/Aktuelles/Auswertung_Statistik_2016.pdf (as per 11.08.2017).

[6] "Hamburg braces for G20 violence as tensions rise over police tactics", in: The Guardian, 05.07.2017; URL: https://www.theguardian.com/world/2017/jul/05/hamburg-braced-for-huge-violent-protests-in-run-up-to-g20-summit_ (as per 16.02.2018).

[7] "Arrests and injuries as Hamburg gripped by mass anti-G20 protests ", in: The Guardian, 07.07.2017; URL: https://www.theguardian.com/world/2017/jul/07/g20-protests-hamburg-altona-messehalle (as per 16.02.2018).

[8] "Violence on Hamburg streets as G20 protests descend into chaos", Video, in: The Daily Mail (Mail Online); URL: http://www.dailymail.co.uk/video/news/video-1496997/Violence-Hamburg-streets-G20-protests-descend-chaos.html_(as per 16.02.2018).

[9] "Police investigate deadly Berlin truck crash as 'presumed terrorist attack' ", in: The Guardian, 20.12.2016; URL: https://www.theguardian.com/world/2016/dec/19/berlin-truck-crashes-into-christmas-market (as per 16.02.2018).

[10] "Terror in Berlin How the Attack Has Changed the Country", in: Spiegel Online, 23.12.2016; URL: http://www.spiegel.de/international/germany/berlin-terror-reconstruction-of-the-breitscheidplatz -attack-a-1127251.html_(as per 16.02.2018).

[11] "Deutsche Telekom upgrades wiretapping protection in mobile communications", 12.09.2013; https://www.telekom.com/en/media/media-information/archive/deutsche-telekom-upgrades-wiretapping-protection-in-mobile-communications-360314 (as per 21.02.2018)

[12] "26/11 Mumbai terror attacks: Here's what happened at Taj Mahal Hotel, Trident-Oberoi, Nariman House", The Indian Express; http://indianexpress.com/article/26-11/timeline/2611-mumbai-terror-attacks-heres-what-happened-at-taj-mahal-hotel-trident-oberoi-nariman-house/ (as per 21.02.2018)

[13] Drucksache 18/10598 vom 09.12.2016 des Deutschen Bundestages, Seite 9.

[14] Welt: Bayern: Während Amoklaufs fiel der Polizeifunk minutenlang aus; URL: https://www.welt.de/regionales/bayern/article158909962/Waehrend-Amoklaufs-fiel-der-Polizeifunk-minutenlang-aus.html (as per 06.08.2017)

[15] Kölner Stadt-Anzeiger: Polizeibeamter berichtet: Funknetz war in der Silvesternacht zeitweise ausgefallen; URL: http://www.ksta.de/politik/polizeibeamter-berichtet-funknetz-war-in-der-silvesternacht-zeitweise-ausgefallen-24380364 (as per 06.08.2017)]

[16] RTL Info: Attentats à Bruxelles: voici pourquoi la police a dû communiquer via Whatsapp pendant les opérations de secours; URL: https://www.rtl.be/info/belgique/faits-divers/attentats-a-bruxelles-voici-pourquoi-la-police-a-du-communiquer-via-whatsapp-pendant-les-operations-de-secours-805347.aspx (as per 21.02.2018)

[17] Rundfunk Berlin-Brandenburg: Nach Störungen beim Digitalfunk: Berlin will für seine Polizisten 16.000 Handys kaufen; URL: https://www.rbb-online.de/politik/beitrag/2017/03/berlin-polizei-handys-polizeifunk.html (as per 06.08.2017)

[18] Real Time Cryptanalysis of A5/1 on a PC; by Alex Biryukov, Adi Shamir and David Wagner; URL: https://cryptome.org/a51-bsw.htm (as per 23.02.2018)

[19] Promoting the Digitization of Japanese Fire Prevention/Emergency Wireless Communications Systems; by Kawabata Masaaki; NEC Technical Journal／Vol.8 No.1／Special Issue on Solving Social Issues Through Business Activities, p 53-58, downloadable at https://www.nec.com/en/global/techrep/journal/g13/n01/pdf/130112.pdf (as per 5.05.2018)

Relevance for the Danube Region

DOI: 10.24989/ocg.v331.41

This section details the relevance for the Danube Region for those contributions that do not immediately relate to the Region. The following texts were provided by Robert Müller-Török und Alexander Prosser.

DIGITAL GOVERNMENT AS SERVICE DELIVERY FOR DIFFICULT TERRITORY
A CASE STUDY OF BONIN ISLANDS

Hiroko Kudo

The paper analyses the role of digital services in the development of regions which are either economically disadvantaged and/or not connected to the main axes of traffic with a special view of regions encompassing both regions that are economically advantaged and disadvantaged. The paper discusses research results from the indo-pacific region, however, these results directly translate into the Danube Region, where "old" economically advantaged and reform regions can be found. Here and there, the levelling of these economic and infrastructural differences is a key political topic. The paper describes how digital services, with a special view to smart city services, may contribute to this economic development process in the less advantaged regions.

The paper also stresses the relationship between "physical" infrastructure development and said digital services giving examples. The conclusions drawn are very similar to the conclusions by Tirziu/Vrabie and Schenk/Laue. Particularly the role of Business Intelligence and Internet of Things infrastructure is pointed out; the research results provide an interesting and stimulating analogy to the Danube Region.

THE SHOPPERS; VENUE SHOPPING, ASYLUM SHOPPING: A RESOLUTION IN EURODAC?

Catherine Odorige

The topic of asylum seekers and the abuse of the right to asylum are stringent topics in the Danube Region. Asylum shopping and waves of migrants moving throughout the Danube Region towards wealthy places, such as Germany or Austria constitute a problem that threatens to undermine the political cohesion in the Danube Region. Also the internationalisation of migration and asylum control policy in the framework of venue shopping stringently applies to the Danube Region.

The paper presents EURODAC, an automated biometric identification allowing for instant and exact comparison of unique physiological features for individual's iris, face and finger print for law enforcement purposes of illegal migrants. EURODAC can therefore be a viable solution to detect and furthermore prevent asylum shopping throughout the Danube Region.

DIGITALISATION VS. INFORMATIZATION: DIFFERENT APPROACHES TO GOVERNANCE TRANSFORMATION

Alois Paulin

The paper analyses the relevance of the informatisation for the public sector in view of the "4.0" debate, that is the steps from mechanisation to automation to digitisation to informatisation. The discussion originated in the private – mainly manufacturing – sector, but also applies to smart cities and other domains of public ICT (see the paper of Prosser in this volume).

The paper then stringently argues how the step from digitisation to informatisation transforms real-world governance structures. This is an effect that can be observed in the Danube Region (see for example the paper of Nemeslaki); on the other hand, failure to change governance structures may stop the digitisation, for a negative example from Baden-Württemberg, see the paper of Schenk/Giesbrecht.

The paper then introduces the concept of "governance informatisation" utilising the technologies to overhaul governance as such and to adapt it to the present-day infrastructure. This is actually one of the "opportunities" cited by Grecu et al. in their paper. It may provide stimulus to overcome the impasse in the case described by Schenk/Giesbrecht.

BIG DATA AND ALGORITHMS IN THE PUBLIC SECTOR AND THEIR IMPACT ON THE TRANSPARENCY OF DECISION-MAKING

Gergely László Szőke

The paper provides a stringent discussion on how real-time, transaction data-based business intelligence may transform a public sector organisation. This transformational aspect alone makes it highly relevant to the Danube Region (the paper is from a Hungarian author, yet deals with the topics on a general level). The paper actually deals with a similar domain as the contribution by Petrov/Petrov from Moldova describing and analysing very similar effects in the Moldovian context.

Of course, the transparency is limited mainly by the General Data Protection Regulation, which is stringently outlined by the paper. Here the paper may be read in conjunction with the contribution of Orbán analysing the limitations of open government data in Hungary.

CYBERSECURITY IN THE EUROPEAN UNION

Andreas Düll, Anja Schoch and Matthias Straub

The contribution describes the EU framework for cyber defence and resilience. The description is necessarily on a general, EU-wide, level, nevertheless the Danube Region is particularly prone to cyber-attacks, not only due to the small scale of most of the countries, which prevent utilisation of scale effects in cyber-defence measures, but also due to the specific risk exposure of the region. In this connection, this paper is related to research presented in this volume by Szádeczky describing the corresponding initiatives and frameworks in Hungary.

However, the paper concludes that “[t]he Commission's strategy does not contain any comprehensible criteria that could shed light on which instruments should be used”, which is particularly disappointing for the countries of the Danube Region, which would benefit from a standardised EU-wide framework. The work of the European Cybercrime Centre is analysed and here opportunities for the (on average) smaller countries of the Danube Region for utilising scale effects arise. Such work can provide valuable input, for instance, for the cyber-defence activities at one of the conference host institutions, the University of Public Service.

IMPROVING DISTRIBUTED VULNERABILITY ASSESSMENT MODEL OF CYBERSECURITY

Kálmán Hadarics and Ferenc Leitold

The contribution analyses the Vulnerability Assessment Model in cyber-security; it links up with the papers by Düll et al. and Szádeczky in this volume. It provides a modelling framework for the elements of cyber-defence; a particular merit is the broad range of cyber-attack types. This modelling framework could be a valuable input to the cyber defence education and research centre that is currently being built up at the host institution of the conference. It reflects the need for a scalable, effective cyber defence system for the – on average – small and medium-sized countries in the region.

Of particular interest is the inclusion of human factors in the model. The relevance for the Danube Region is the identification of needs for capacity building in the pertinent fields and can provide research-based input in programme definitions of institutions, such as EUSDR PA10 and similar frameworks.

OTT REGULATION A WAY OF COMBATING CYBERCRIMES

Veronica Mocanu

The paper deals with Over-the-Top (OTT) services, that is the distribution of television or radio over the Internet without the control of a network operator. Today, this mainly concerns international players, such as youtube, HBO or Netflix; however, in the future as the technology will mature, also local/regional service providers are almost bound to emerge. This is particularly true for services in local language. This may happen in the framework of local subsidiaries of international organisations or genuinely regional players. Due to ethnic minorities in the Danube Region, such local-language services will automatically generate considerable cross-border traffic. All the regulatory issues brought up by the paper apply.

The paper analyses a number of risks for OTT services that equally apply to regional service providers. A solution in this regard may be provided by the regulatory framework of the European Union, which is presented in the paper. Due to the territorial, legal and language fragmentation that directly affects OTT services, such regulatory framework is immensely useful for the Danube Region.

EGOVERNMENT AS AN ELEMENT OF THE RIGHT TO GOOD ADMINISTRATION

Justyna Matusiak and Marcin Princ

The contribution "eGovernment as an element of the right to good administration" by Justyna Matusiak and Marcin Princ establishs a link between eGovernment and the EU Charter of Fundamental Rights. When we have a look on e.g. the current processing times of the German Administrative Courts, which are ipso facto dead-locked by migration and asylum cases, it appears evident, that in times of increased absolute administration process figures the whole administrative process must be streamlined, namely by means of eGovernment. The issue is very relevant for the Danube Strategy Countries, simply because migration and asylum issues are tied to the famous "Balkan Route", which goes along the Danube from Moldova and Bulgaria to Germany. Poland is, much to our dismay, not within the Danube Strategy, but it belongs both to CEE and to the Visegrad Group, hence parallels between Polish and Danube administration may be drawn. The main finding of the paper, that "eGovernment regnorum fundamentum", is very applicable in all the Danube Strategy Countries.

ECOHESION: HOW TO MEASURE THE MAIN DRIVERS OF ADMINISTRATIVE BURDEN REDUCTION

Tamás Laposa

The same topic is covered and, more than that, dealt with at a more detailled level by "ECOHESION: HOW TO MEASURE THE MAIN DRIVERS OF ADMINISTRATIVE BURDEN REDUCTION" by Tamás Laposa. His eCohesion is derived from Regulation 1303/2013 which defines Electronic Data Interchange, Interoperability and the Once-only-principle as the fundaments of applied eGovernment. So whilst Justyna Matusiak and Marcin Princ answer the "Why", Tamás Laposa answers the "How". Namely interoperability is, in a Danube Region where no large domestic state exists, but borders every 50 kilometers, the name of the game. Without eCohesion the Danube Region will be as divided as Germany before the "Deutscher Zollverein", i.e. a totally divided country with independent administrations and massive burdens for citizens, businesses and also administrations. Laposa also provides evidence for cost benefits, an issue very relevant to most of the Danube Region Countries.

GLOBAL IDENTITY MANAGEMENT FOR INDIVIDUALS? THE RIGHT TO BE FORGOTTEN AND ISSUES OF EXTRATERRITORIALITY

Petra Lea Láncos

Petra Láncos provides a different topic, which is strongly relevant for all EU Member States and for the Candidate States of the Danube Region. Her contribution "Global identity management for individuals? The right to be forgotten and issues of extraterritoriality" deals with the EU General Data Protection Regulation, which will enter into force shortly after the conference, on May 25th, 2018. Due to the trend of moving sensitive applications to smaller countries with a more favorable jurisdiction, the topic is very relevant for the Danube Strategy Countries. Enterprises like gmx.de or Facebook can easily switch server locations and try to avoid e.g. a Legislation and Jurisdiction in Spain by moving to Moldova or Romania. The solution pointed out by the French Constitutional Court seems very applicable in this context.

REVISITING OPEN DATA RESEARCH THROUGH THE LENS OF THE DATA VALUE CHAIN

Csaba Csáki and Andrea Kő

The contribution "REVISITING OPEN DATA RESEARCH THROUGH THE LENS OF THE DATA VALUE CHAIN" deals with the topic of Open Data in General and Open Government Data in particular. In the traditional western-european countries it is not known that many Open Data laws and Freedom of Information Acts were issued after the fall of the Iron Curtain, whilst developed western states like e.g. Bavaria or Baden-Württemberg got such legislation either decades later or not yet. So it seems more than valuable to gain from the vast experience the two authors have. The value chain seems to be a very interesting progress in that context and should be widely shared.

RESEARCHERS AS MEDIATORS BETWEEN POLICYMAKERS AND PRACTITIONERS – DO THEY HAVE THE NECESSARY SKILLS?

Adriana Zaiţ

Her contribution "Researchers as mediators between policymakers and practitioners – do they have the necessary skills?" questions the self-perception of scientists, a topic very appropriate at an international conference of researchers. Especially nowadays, where scientists are appointed ipso facto as referees on so-called "fake news" and asked questions politicians can either not answer or are not believed if they try to answer, this issue becomes very important. Her research shows that there is, especially in Romania where the study took place, room for improvement of skills of researchers. We believe sincerely that her results are applicable all over the Danube Region.

THE PERMANENT CAMPAIGN IN SOCIAL MEDIA: A CASE STUDY OF POLAND

Dorota Domalewska

"War is the father of all things" of ancient Heraclitus could be the first thought when Dorota Domalewska from the War Studies University of Poland presents us with her contribution "THE PERMANENT CAMPAIGN IN SOCIAL MEDIA: A CASE STUDY OF POLAND". Based on a a study in her native Poland she presents us with impressing findings which could change our perception of politics and political campaigning. The election campaigning seems to become a permanent institution, not restricted to the few months before elections any more. Her insights into politicians using Twitter are highly relevant for the Danube Region Countries, especially those with a higher level of political discourse or a higher percentage of active politicians. And even the sitting US President can probably be better understood after having read this study.

Indices

INDEX OF AUTHORS

DOI: 10.24989/ocg.v331.42

INDEX

DOI: 10.24989/ocg.v331.43