E-GOVERNMENT, TRANSPARENCY AND PERSONAL DATA PROTECTION. A NEW ANALYSIS' APPROACH TO AN OLD JURIDICAL ISSUE

Annarita Ricci[1]

Abstract

In recent years, many governments increased transparency, publicity and free access in their activities. Information and communication technologies (ICTs) are seen as a powerful tool to reduce "public diseases" such as low citizen trust, bad performance, low accountability and corruption. While some of these efforts have received a considerable attention, the balance between the value of transparency and the necessity of protecting individual's personal rights has not been widely considered. It is an obvious fact that administrative records and documents may contain personal data, so it has become necessary to guarantee citizens' privacy and respect the principles set forth in the European legislation. Information can indeed become more damaging if spread on the web rather than through conventional channels. Therefore, personal identity has to be protected through the removal of information which it is no longer necessary to process.

In this scenario, the present work analyses the main measures public administrative bodies are required to implement, regardless of the purposes for which the information is posted online.

The analysis conducted will be a scholar reflection based on Directive 95/46/EC and recent "Regulation (EU) 2016/679 of the European Parliament ad 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)". The paper will introduce a perspective concerning three different topics, namely the right to personal data protection, the data quality and the principle of proportionality. The road map will be as follows: to clarify the notion of data quality, to analyze the link between this principle and the value of transparency of public administrative activities and finally to introduce the dimension of the protection of personal data as a relative and not as an absolute right.

1. Information as a personal identity component. Information as a "common good"

Web has become an extraordinary communication instrument and, as such, an important tool for Public Administrative Bodies (PAB) to ensure widespread knowledge of the information concerning organizational features of their own. The knowledge ensures transparency, enabling wide-ranging supervision of the PAB's capacity to achieve the respective objectives as well as of the mechanism in place to assess civil servants' performance. Publishing details about public sector subjects' private interests is part of a range of measures used to manage potential conflicts of interest and to increase accountability. It would be, however, oversimplistic to assume that the transparency is (only) a control instrument. The transparency is much more, guaranteeing the

[1] Department of Juridical and Social Sciences, University G.d'Annunzio (Italy), annarita.ricci@unich.it

citizens participation in public life[2]. Citizens, through the implementation of the transparency principle, participate in the public interest selection. In other words, through the transparency, sovereignty has declined in administrative proceedings. Impartiality, transparency and professional conduct amongst public sector subjects is recognized as a key to ensuring excellence and quality in the performance of relevant public positions. Then, the use of Information Technologies (IT) improves efficiency of public services, reducing the distance felt by citizens towards the public administration. For example, a city hall portal enables citizens to interact online with the PAB, supplying information and applying for services without the costs of face-to-face and manual form processing [3].

Going now beyond the intuitive chance of IT, it is necessary to note that the balance between the use of IT and the necessity of protecting fundamental personal rights becomes particularly tricky. Indeed, information may contain personal data and, additionally, sensitive data and it is a fact that personal data constitute a fundamental component of the individual personal identity[3]. It is also well known that incomplete or incorrect information could have negative repercussions on the personal identity. At the same time, outdated information which does not represent the reality, can provide a representation of the individual which is untruthful or out of context. Hence, it becomes necessary to refer to the right to personal data protection as a complex instrument of the data subject's safeguard and, at the same time, of the controller's accountability[4]. So, to understand these concepts (protection of the data subject as the weak party of the relation and accountability), apparently contrasting, and their role as key elements of, as called in the legal literature, the "proactive approach to privacy" [4], it is useful to illustrate briefly the very essential points of the European legal framework.

We have to start from the rules set forth by the 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[5]. It may appear superfluous to recall the Directive 95/46/EC, considering its repeal following the entry into force of the recent Regulation (EU) 2016/679 (General Data Protection Regulation or more simply GDPR); however, the operation is necessary to define the *ratio* of the personal data processing regulation.

The Directive 95/46/EC described an innovative model that has influenced decisively the approach of the European Legislator to the personal data protection: a model that has led to the transition from a protection guaranteed only in the case of information collected in automated form to a wider protection that includes all operations performed upon personal data, regardless of the methods adopted and the instruments used and, above all, based on a need of balance, as well expressed in the title "Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data". The real novelty of the European harmonization of the rules of personal data protection, started with the Directive 95/46/EC, is the recognition of the

[2] As stated by the recent Opinion 02/2016 on the publication of Personal data for Transparency purposes in the Public Sector, adopted on 8 June 2016 by Article 29 Data Protection Working Party: "the notion of transparency is linked with the principles of openness, good administration and good governance as enshrined in the Treaties (Articles 10 and 11 of the Treaty on European Union and Articles 15 and 298 of the Treaty on the functioning of European Union) and in the Charter of Fundamental Rights of the European Union (Article 41)".

[3] The term "identity", in this paper, refers to all personal attributes of the individual as a whole. In essence, it could be argued that identity is the uniqueness of each individual that distinguishes him/her, differentiating him/her from the others, and representing him/her in his/her diversity. On the notion of identity, as stated in this work, see [14].

[4] For the personal data protection's dimension as a fundamental right in European law, see: [6] [7] [9] [10] [11].

[5] Referring to the content of General Data Protection Regulation, Kuner use the emblematic term of "copernican revolution": see [8].

personal data value as information necessary for the functioning of the economic and social life. To point out this element, it is sufficient to consider some of the Recitals of the Directive: "whereas the economic and social integration resulting from the establishment and functioning of the internal market (...) will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called (...) to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market (Recital no. 5)" it is necessary "to remove the obstacles to flows of personal data", enhancing that "the level of protection of the rights and freedoms of individuals with regard to the processing of such data be equivalent in all Member States" (Recital no. 8).

Data processing is qualified as an essential element of economic and social progress, which must be ensured in respect of the rights and fundamental freedoms of individuals. It is a "principle of guarantee" that the data processing systems, being at the service of the person, must respect. In essence, the aim of the Directive 95/46/EC (as well as of the Regulation) -which must be kept in constant consideration to avoid the risk of distorting the meaning of the related provisions- is to maintain the balance between the free movement of personal data and the protection of the rights and freedoms of the person. The balance of the interests is innate to the complex nature of personal data: an essential element for the free movement of persons, goods and services and a personal identity component. It is the balancing of the interests to justify, for example, the irrelevance of data subject's consent for the lawfulness of the personal data processing, whenever the operation is instrumental to the execution of a task of public interest (art. 7, lett. f) of the Directive, confirmed by art. 6 (1), lett. e) of the GDPR.

2. The principle of "data quality"

The article 6 of the Directive 95/46/EC lays down the related rules to ensure the accuracy, completeness, relevance of the data processed and that they are not excessive in relation to the specific purpose pursued by the processing. Only such data shall be processed as are "adequate, relevant and not excessive in relation to the purpose for which they are collected or further processed" [2].

The purpose must have been specified in advance and made manifest by the controller to the data subject prior to, and in any event, not later than, the time when the collection of personal data occurs. The processing of personal data for undefined or unlimited purpose is unlawful. Specification of purpose is an essential first step in applying data protection laws and designing data protection safeguards for any processing operation. Indeed, specification of the purpose is a pre-requisite for applying other data quality requirements, including the adequacy, relevance, proportionality and accuracy of the data collected and the requirements regarding the period of data retention. The principle of purpose limitation -designed to establish the boundaries within which personal data collected for a given purpose may be processed and may be put to further use- is structured along two coordinates: the controller must inform the data subjects of the processing purposes (transparency) and data processed for one or more declared purposes may not in general be used for other purposes (limitation).

The principle of transparency requires that the purposes of the data processing are well defined and comprehensible for an "average" data subject without expert legal or technical knowledge[6].

According, instead, to the principle of limitation, legitimate processing is limited to its initially specified purpose and any new purpose of processing will require a separate new legal basis. The categories of data chosen for processing have to be necessarily specified in order to achieve the declared overall aim of the processing operations, and a controller should strictly limit collection of data only to information *directly* relevant for the specific purpose of the processing[7]. Let us take as an example a statement of the Italian Data Protection Authority (order dated September 7, 2011). In this case, the Italian Data Protection Authority has banned an online University from processing personal data of students collected in an online form that was used to remain constantly informed about the activities of University. As evidenced by the order, the online University processed also information -such as date and place of birth, social security number, citizenship- that were not relevant to the purposes of the processing. In addition to the ban from processing the irrelevant data, Authority has prescribed to change the mode of personal data collection, eliminating from the registration form the data that resulted excessive in relation to the aims pursued.

The principle of legitimate purposes limitation goes hand-in-hand with the principle of data minimisation. According to this principle, the processing of personal data is permitted only if it is required to achieve a specified purpose: if this scope can be accomplished with anonymous or pseudonymous data, then this latter modalities should be preferred [1] [5] [13]. In order to prevent unnecessary and potentially unlawful data processing, data controller must carefully consider which data are strictly necessary to perform the processing purposes, and erase data when those purposes have been served. The principle of data minimisation, not specified in the Directive 95/46/EC, is explicitly provided by Article 5 (1) lett. (c) of GDPR. According to this provision, personal data shall be "adequate, relevant and *limited to what is necessary* in relation to the purposes for which they are processed". This therefore also entails that data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data at all, or as few personal data as possible. As already pointed out, the accuracy of data, including updating, is an absolute necessity, in light of the potential damage that might be caused to the data subject due to data inaccuracies. Only information that is qualitatively correct, provides a correct representation of the individual [12]. If it is true that only accurate information provides a valuable instrument to protect fundamental rights, at the same time the requirement of completeness and updated collection of information may be a relevant instrument to prevent the creation and diffusion of untrue,

[6] The importance of the principle of transparency is crucial for the personal data protection. As stated in the Recital no. 39 of GDPR: "it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used". Therefore, it is evident that through transparency the right to protection of personal data is recognized as right to informational self-determination and the data subject can exercise an effective control over his/her personal identity.

[7] On April 2, 2013 the WP29 provided an opinion on the principle of purpose limitation. The opinion analyses both components ("building blocks", in the words of the WP29) of the purpose limitation principle: (1) purpose specification; and (2) compatible use, or the requirement that any further processing must be compatible with the original purpose for which the personal data were collected. After stating that the "compatible use" requirement needs to be assessed on a case-by-case basis, the opinion points out the key factors that should be taken into account in this analysis: the relationship between the purposes for data collection and the purposes for further processing; the context in which the data have been collected and the reasonable expectations of the data subjects regarding further use of the data; the nature of the data and the impact of the further processing on the data subjects; and the safeguards put in place by the data controller to ensure fair processing and prevent undue harm to data subjects.

incomplete, or outdated information, likely to create untrue opinion, up to being discriminatory. These considerations may assume a significant importance if contextualized in the digital world, where it may be very difficult to remove an incorrect information. The time factor becomes then relevant, and likewise the analysis of elements such as the purpose of the data processing and of the (particular) context of the purpose of data processing.

Therefore, it is necessary to guarantee the limited retention of data principle. This requires ensuring that the period for which the personal data are stored is limited to a strict minimum. This is a procedural rule that formalizes the principle of limitation purposes. The processing and the data that are the object of the processing are linked to a specific aim, and it is on this relationship of necessary instrumentality that the legitimacy of the operations is based. It is irrelevant whether personal data (in the association between the name and other information) assume a derogatory nature or, more generally, is invasive of data subject's personal identity. What is relevant is the function of the original collection of personal data, or the purpose declared by the data controller: if these are no longer in effect, personal data must be erased. If it is evident that this rule derives from the said above "data minimisation" principle, the operation to determine the "expiration time" of a processing of personal data is not so obvious. The time limitation for storing personal data applies, however, only to data kept in a form that permits identification of data subjects. Lawful storage of data that are no longer needed could, therefore, be achieved by anonymization of the data.

3. Quality of Information as a multi-dimensional principle

We can assume that quality of information is one of the key criteria of data protection. The legitimacy of the data is subject to compliance with this general principle, representing the most important element for protecting personal identity. As said, this principle includes the following rules: "limitation", which prohibits the processing of personal data "in a way incompatible" with specified and known (by data subjects) purposes; "limited retention or storage limitation", which requires the deletion of personal data that are no longer necessary to achieve the objectives of the processing of the data; finally, "data minimization", which requires that every data controller limits much more strictly the amount of data they collect. As said before, the Article 5 of GDPR confirms the principles according to which personal data may be processed, only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected. Nevertheless, General Data Protection Regulation emphasizes data minimization principle and value of transparency, rules that have to be calibrated to the status of the data subject.

It is necessary to point out another element. The respect of data quality rules goes hand-to-hand with the principle of accountability. The controller has to ensure that only accurate, complete and up-to-dated data are processed. Every reasonable step must be taken to ensure that data that are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. A critical element can be established: the "reasonable measures". The concept of reasonableness may appear indeed vague. It is possible to discuss its content in the light of the general criteria listed by GDPR: the nature of data; the data processing purposes; the preliminary and necessary analysis of the data processing risks and the state of the art of the knowledge about technical security measures. Therefore, some useful tools may consist of checks at the time of collection, periodic checks or use of a software that prevents the acquisition of incomplete, irrelevant, or inaccurate data.

It is clear that the rule framework appears complex and some requested measures may be hard to adopt, but we can consider unquestionable the following element. There is a need to stress the

accountability -and the GDPR goes in this direction- requiring data controller's awareness of the nature and the purposes of the processing, and also of the risks of the data processing: therefore in practice, a preliminary analysis of the context. Therefore, PBA, as data controllers, must consider processing within organizations separately from the purpose of publishing personal data. Then, when deciding whether to make information containing personal data available on-line, PBA should always bear in mind the consequences of doing so. It is much more than a responsibility issue. It is a selective approach to personal data protection, differentiating between different nature, cases and purposes, and taking into account specific situations with regard, for example, to the content of the personal details being published. In essence, different methods of processing data for different contexts. In this way, the fulfillment of the proportionality requirement can be effectively assured. Applying this approach, also the period for retaining personal data should be determined according to the legitimate purposes for which they are held. So, processing within competent institutions should be considered separately from the purpose of publishing personal data.

4. An attempt to a selective approach. The Italian Data Protection Authority's Guidelines for the personal data processing by Public Administrative Bodies for publicity and transparency purposes

In 2014 the Italian Data Protection Authority established specific guidelines to be complied with by PAB when posting administrative records and documents that contain personal data, in order to avoid the violation of citizens' and employees' privacy, and to respect the above described data quality principle. The Guidelines point out a very specific set of arrangements PAB are required to implement regardless of the purposes for which the information is posted online (transparency, publicity, access)[8]. First of all PAB may post, on their official website, records and documents containing personal data only if this dissemination is determined by law or by a regulation. The publication must be appropriate in order to attain the objective pursued, and not go beyond what is necessary to achieve it. Then, PAB have to distinguish the nature of the data. Non-sensitive personal data, for example name and surname, can be published in compliance to the data quality principle. Sensitive or judicial data can be published if supported by a specific legal basis and always taking into consideration the appropriate balancing between data protection and the legitimate public interest[9]; health or sexual orientation data cannot be in any case published. On the contrary if there is not a law or a regulation that allow personal data publication in the website, the publication is legitimate only if data is anonymized. On this last element, the Guidelines states that, in order to anonymize a document, it is not adequate to replace the name with the initials of the person, but it is necessary to completely obscure the name and other information related to the person that may allow identification.

The other main rules stated by the Guidelines can be summarized as follows:

[8] See Article 29 Data Protection Working Party, Opinion 02/2016 on the publication of Personal data for Transparency purposes in the Public Sector.

[9] According to Article 4 (1), lett. d) of the legislative decree no. 196 of 30 June 2003 (Personal Data Protection Code), sensitive data consists of "personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life"; the following lett. e) defines as "judicial", "personal data concerning the criminal record office, the register of offence-related administrative sanctions and the relevant current charges, or the status of being either defendant or the subject of investigations".

- appropriate technological measures should be taken to prevent the online information from being erased, changed or extrapolated;

- the documents should be retrieved, if possible, by way of internal search engines, whilst the indexing of such documents by external search engines should be limited. Relying on internal search engines can ensure that access will be consistent with the purposes for which the information was disclosed as well as preventing the data from being tampered with or taken out of their context;

- the data must remain available for a period no longer than what is necessary in accordance of the sector-related legislation;

- alert systems and software should be deployed to prevent reproduction and re-use of the files containing personal data; such systems can detect and report any dubious access to take the adequate countermeasures.

Therefore, in conclusion, we can say that the Guidelines confirmed the selective approach to the personal data protection. Considering the particular context, the Italian Data Protection Authority has strengthened PBA's duties as data controllers, by improving technical measures of security and control mechanisms by default.

5. Absoluteness and relativity of the right to personal data protection. Recital 4 of the General Regulation Data Protection

In this scenario, Recital no. 4 of the GDPR assumes a very significant relevance. According to this provision: "the processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity". The provision is clear: the right to personal data protection is absolute, considering that it is recognized to anyone; it is relative, considering the possible external constraints that restrict or limit the exercise of the right. In other words, relativity should be referred to the content of the right to personal data protection, that is to all claims that can be exercised by the data subject, not to the right as such. The content of the right is relative since data subject's powers may be restricted, in light of the necessary balancing between individual interests and collective values. The assumption that the exercise of the right to protection of personal data may be restricted -even if it assumes an emblematic relevance given its location in an initial Recital of the GDPR[10]- is not new in the European legal framework about personal data protection. In relation to the right to privacy, to which, as is well known, the right to protection of personal data is linked by a bond of interdependence, Article 8, (2) of the European Convention on Human Rights provides the possibility of authorities' interference for reasons of public interest. Similarly Article 9, (2) of the

[10] The recitals aren't a mere introduction to the legislative text, but a part essential for its understanding and application. See Court of Justice, 25 October 2011, eDate Advertising, C-509/09 and Martinez, C-161/10, par. 54 e 55, available at *http://curia.europa.eu*.

Convention on the Protection of Individuals in regard to the Automatic Processing of Personal Data admits the possibility of restrictions of the right, in case these are necessary measures "protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences, data subject or the rights and freedoms of others". The need to operate a balance between individual and collective interests is expressed also by art. 52, (1) of the Charter of Fundamental Rights, which states that: "any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others". The provision, significantly entitled "Scope and interpretation of rights and principles", states that the rights recognized by the Charter, although relating to the protection of the personal freedom dimension, may be subject to limitations justified by public interest purposes. Then, it is the "relational nature" of the rights that justifies the possible restriction of their content in light of a general interest. It is the social need that goes beyond the individual prerogative, legitimizing powers' restrictions; so in this restriction, the right, a fundamental claim of the individual, sees affirmed its social dimension limited by the relationship with others. These considerations do not call into debate the substance of the right, but its concrete activity in relation to aims that exceed the individual dimension. Restrictions must be reasonable, commensurate to the purpose and their effects must be proportionate in regard both to the benefits and prejudices derived from them.

As said above, after providing that the right to protection of personal data is not an absolute right, Recital no. 4 of the GDPR adds that "this right must be considered in relation to its function in society". What does it mean that the right to protection of personal data should be considered in relations to its function in society? The "function" (which must be taken into consideration) must be referred to personal data. From an ontological point of view, the function is related to the right to protection of personal data, similarly to what happens for the right to property. It is a limit to the owner's claims, justifiable in the light of the object of the right. If the data can have a purpose that is external to the individual dimension of the data subject, or if it can have an impact on the other individuals' fundamental rights, or also if its processing is instrumental to social needs, then the fullness of the claims may be subject to a restriction. In summary, if the personal information is functional to satisfy an interest that goes beyond the boundaries of the "individual interest" of the data subject, it is legitimate and necessary to effect a limitation of the prerogative on the same data. Then, the expression "function in society" appears as the criterion of argumentation in which it is possible to decline the relativity established for the right to personal data protection.

Concluding, we can say that Recital no. 4 of GDPR confirms the above-illustrated system built by the Directive 95/46/EC and the determination argued by the European Court of Justice since the 70s[11]. The decisions of the European Court of Justice may then have been taken having in mind the abstract possibility that the (full) protection of a right, albeit a fundamental one, may have to be balanced with the need of ensuring economic freedoms[12]. The fundamental rights are not on an insuperable level of abstract inviolability. In other words, except for the right to life, other

[11] Court of Justice, 17 December 1970, Internationale Handelsgesellschaft, C-11/1970, available at *http://curia.europa.eu*; Court of Justice 14 May 1974, Nold Kohlen-Und Baustoffgrosshandlung, C-4/73, available at *http://eur-lex.europa.eu*. According to this last decision: "if rights of ownership are protected by the constitutional laws of all the Member States and if similar guarantees are given in respect of their right freely to choose and practice their trade or profession, the rights thereby guaranteed, far from constituting unfettered prerogatives, must be viewed in the light of the social function of the property and activities protected thereunder".

[12] Cass. civ., 17 luglio 2015, n. 15096, in *Giur. it*., 2015, p. 2651.

fundamental rights do not have an absolute value, but instead they a relative one, that may be declined along the coordinates of the proportionality. The need of balancing is justified in light of the individual's social dimension and the consequent reasonable equilibrium between idiosyncratic and collective dimensions.

A good opportunity to assess the repercussions of the proposed reconstruction is offered by a recent decision of the Italian Supreme Court of Cassation[13]. The case is related to the publishing - on the companies register of the Italian Chambers of Commerce- of personal data (name and surname) referred to a director of a bankrupted company, despite the previous removal of the company from the same register. The director has obtained in the first instance the deletion from the public register of personal data and compensation for damage. The Supreme Court has stayed the proceeding, submitting to the Court of Justice of the European Union two preliminary questions. The first question is related to the principle of data's limited retention, which requires the anonymization when the time necessary to achieve the purposes of primary collecting is expired. The Supreme Court has asked whether this principle should prevail over the rules about legal registers. The second question concerns the interpretation of Article 3 of the "First Council Directive 68/151/EEC of 9 March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community". The Supreme Court has asked if that provision enables the restriction of the publishing time in the companies register.

It is not possible here to consider thoroughly the Supreme Court decision. What can be said, however, is that the data registered in the public list are peculiar information in light of their function. These are economic information, subject to a system of advertising, whose free access guarantees the functioning of the market and protects the fairness of the relations established therein. Then, it is necessary to balance the right to personal data protection with the right (of third parties) to certainty of economic relations and business arrangements. Therefore, the right to protection of personal data may be subject to a restriction of content that translates into an impossibility to obtain the cancellation of the data from the public register.

6. Conclusion

The respect of personal data protection right is essential to guarantee democracy. It also true that enhancing data processing is relevant for economic and social progress. Moving from the assumption on the social connotation of personal data, this paper has delivered an overview of the current (related) European legislation, in order to demonstrate that if the data processing is instrumental to social needs, then the fullness of the individual right may be subject to a restriction. This paper affirms that data protection rules should be interpreted and consequently implemented in light of a necessary balance. It could be argued that personal data protection must be, on the contrary, strengthened and not limited, but this is may be misleading. Privacy and personal data protection should be incorporated in a selective approach in which the social function of the data, the processing purposes and the features of the data subjects acquire a particular relevance. By doing so, the duties (as well as the responsibilities) of the data controller will be improved, requiring to adopt internal procedures and implement specific measures, designed in light of the purposes and other above mentioned features, so to implement data-protection principles in

[13] Court of Justice, 12 June 2003, Eugen Schmidberger, Internationale Transporte und Planzuge v Republik Österreich, C-112/00, available at *http://eur-lex.europa.eu*.

advance. This is the direction of the recent GDPR that is, moreover, drawn in accordance with the aforementioned approach taken by the European Court of Justice to the more general subject of fundamental rights.

7. References

[1] AA.VV.: Lessons from the identity trail - Anonymity, privacy and identity in a networked society, Keer I., Steeves V., Lucock C. (ed.), Oxford University Press, 2009.

[2] BOSCO, F., CREEMERS, N., FERRARIS, V., GUAGNIN, D. and KOOPS, B-J.: Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities, in: S. Gutwirth, R. Leenes, P. de Hert (ed.), Reforming European Data Protection Law, Springer, 2015, p. 17.

[3] BROWN, I.: Working Paper no. 1, The challenges to European data protection law and principles, 20 January 2010, European Commission Directorate-General Justice, Freedom and Security, Comparative Study on different approaches to new privacy challenges, p. 9.

[4] CAVOUKIAN, A.: Evolving FIPPs: Proactive Approaches to Privacy, Not Privacy Paternalism, in: S. Gutwirth, R. Leenes, P. de Hert (ed.), Reforming European Data Protection Law, Springer, 2015.

[5] FINOCCHIARO, G.: Anonimato, in: Digesto delle discipline privatistiche, Torino, 2010, p. 12.

[6] FUSTER, G.: The Emergence of Personal Data Protection as a Fundamental Right of EU, Springer, 2014, p. 234 ss.

[7] KROTOSZYNSKI, R. J.: Privacy Revisited. A Global Perspective on the Right to be Left Alone, Oxford Press., 2016, p. 143.

[8] KUNER, C.: The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, in Privacy Security Law Report, 11, 2012.

[9] RODOTÀ, S.: Elaboratori elettronici e controllo sociale, Bologna, 1973.

[10] RODOTÀ, S.: Tecnologie e diritti, Bologna, 1995.

[11] RODOTÀ, S.: Data Protection as a Fundamental Right, in: Gutwirth et al. (ed.), Reinventing Data Protection?, Springer, 2009, p. 78.

[12] RICCI, A.: Quality of Information, Right to Oblivion and Digital Reputation (with G. Finocchiaro), in: B. Custers, T. Calders, B. Schermer, T. Zarsky (ed.), Discrimination in the Information Society, Springer, 2013, p. 289.

[13] RICCI, A.: Anonymity: a Comparison between the Legal and Computer Science Perspectives (with Mascetti S., Monreale A., Gerino A.), in: S. Gutwirth, R. Leenes, P. de Hert (ed.), European Data Protection: Coming of Age, Springer, 2013, p. 85.

[14] ZATTI, P.: Maschere del diritto, volti della vita, Milano, 2009, p. 35.