THE ROLE OF INTERNET INTERMEDIARIES IN COMBATTING CYBERCRIME: OBLIGATIONS AND LIABILITY

Kinga Sorbán[1]

DOI: 10.24989/ocg.v335.1

Abstract
Even though the internet is a very useful asset to everyday life, it can facilitate crime as it can be used to achieve unlawful goals. Stepping up against cybercrime effectively requires extensive international cooperation between law enforcement agencies and the private sector, and between the law enforcement agencies themselves. Internet intermediary service providers such as ISPs, hosting providers and search engine providers are in a special position when it comes to tackling cybercrime: they have to balance carefully between protecting the rights of their users (such as the right to privacy or free speech) and exercising corporate responsibility to prevent and respond to cybercrimes. These providers are sometimes indispensable participants of a successful investigation, because they are the entities that are in a position to provide data to law enforcement agencies and carry out blocking orders. One of the aims of this paper is to give a short overview of those voluntary and obligatory actions that the providers take in order to support the investigative process in Hungary. Besides these actions that stem from the social responsibility and legally enacted obligations, the providers may also be held liable for the actions of third parties (although they may be exempted if certain conditions are met). The second aim of this paper is to analyze the twofold nature of the position of intermediary service providers and to map the arising conflicts between their liability and their role as participants of cybercrime investigations.

1. Introduction

There is a recurring phrase, that comes up frequently in the press and public debates, namely that the smaller and bigger tech-companies shall be involved in ensuring the „lawful" and „proper" functioning of the internet. This statement and the related policies to strengthen state regulation or to facilitate the self-regulation of these enterprises are impressive, but often incapable to live up to the expectations. That is not surprising because one has to overcome serious difficulties already at the starting point when aiming to define what the lawful functioning of a supranational global network – which connects several countries - consisting of thousands of devices is. Which one is the country or international organization that should create the rules that define „proper" functioning? Would we be even capable to create one global legal framework, leading to several nations giving up part of their sovereign rights to share one jointly worded set of community norms? In the past years – as among others Tamás Klein notes [4] – we have come a long way and don't consider the internet a lawless territory anymore, however we still can't recognize the online sphere as *res communis omnium usus*, as the outer space yet. The internet as an infrastructure is a set of standardized technical solutions, which are based on physical and mathematical rationale,

[1] National University of Public Services, 1083 Budapest, Ludovika tér 2., sorban.kinga@uni-nke.hu

therefore rather than ensuring the proper functioning of the internet itself we should concentrate on having an impact on those behaviours that are conducted during the use of the World Wide Web. The behaviours shown while using the internet may be unlawful, they can cause harm to other users and can negatively affect the functioning of the devices that constitute the infrastructure. Therefore, the legitimate use of the infrastructure is usually the cornerstone of the new regulatory initiatives rather than the regulation of the functioning of the infrastructure. If a murder happens in a building, we usually call the police and not the owner of the property. Why would we do differently when a crime happens in the online sphere, where the sole right to deliver justice and inflict punishment on wrongdoers also belongs to the national criminal justice system? Having said this, we also have to note that some of the service providers have such influence over the infrastructure or over some elements thereof, that their involvement is necessary to conduct criminal investigations successfully. Besides the facts that the service providers have to help law enforcement agencies – typically based on their legal obligations –these providers themselves may be held liable for third party information. In an ideal situation, these interests are parallel: by fulfilling their legal obligations to aid the law enforcement agencies the providers also adhere to the conditions of exemption from liability. There may be some situations where the interest of the provider and the law enforcement agencies concur: some providers might not be willing to contribute to the success of the criminal investigations, because if they recognise that they had knowledge of certain information they might lose the possibility to be exempted from liability provided by sectoral legislation. Hungary is a good example to illustrate the theoretical clash between providers' obligations and voluntary measures to prevent or put an end to infringements. The common European liability framework attaches liability to actual knowledge about the illegal information, which might hinder the providers' willingness to prevent and police these infringements on their own. The users may also have some expectations towards the service provider such as the confidential handling of personal data. Stemming from the Data Protection regulation[2] of the EU and the Hungarian Act on the right of informational self-determination and the freedom of information[3] the users shall lawfully expect that the provider handle their personal data confidentially and the providers can be held liable for breaching this obligation. This applies to IP addresses as well, because in the Breyer-case, the Court of Justice of the European Union (hereinafter the CJEU) ruled that dynamic IP address should be considered as personal data.[4] Providers therefore may be reluctant to share certain information on their clients.

The prompt regulation of intermediary obligations and liability is still an open question throughout Europe. There seems to be however a common understanding the service providers certainly have some kind of responsibility, yet the form and scope is still undecided. There is a proposal[5] in front of the legislators of the EU which's main goal is to reform cross-border access to electronic evidence and to enhance cooperation with service providers. As the explanatory memorandum of the proposal highlights, Member States have expanded their national tools resulting in the fragmentation of norms, and conflicting obligations. The proposal was recently criticised for not

[2] 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) OJ L 119, 4.5.2016, p. 1–88.

[3] Act CXII of 2011. on the right of informational self-determination and the freedom of information (Infotv.).

[4] C‑ 582/14 REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 28 October 2014, received at the Court on 17 December 2014, in the proceedings Patrick Breyer v Bundesrepublik Deutschland.

[5] Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Order for electronic evidence in criminal matters.

taking into account the different legal obligations of service providers that already exist.[6] National rules that complement European legal instruments are very important to provide a level playing field for the providers who operate on the European market. These rules are important for law enforcement agencies as well, because pursuant to the proposed regulation these agencies will be able to contact service providers in other Member States directly, therefore having information on and understanding the extent of the providers' exact obligations and the scope of their liabilities in different Member States is of paramount importance in order to conduct a successful procedure.

The aim of this study is to show through the example of one Member State (Hungary) how diverse the obligations and liability of intermediary service providers can be. The paper also highlights those points where the Hungarian regulation differs from the common European norms.

2. The types of intermediary service providers

The term intermediary service provider does not refer to one specific type of provider; it describes a certain legally defined group of actors that provide information society services. For the purposes of this paper it is crucial to make a clear distinction between the different types of intermediary service providers, because each actor has a different relation to unlawful information, therefore their involvement in the investigative process and the existence and scope of their liability may differ. The E-commerce Directive defines the following types of intermediary service providers:

- mere conduit and network access providers
- caching providers
- hosting providers.[7]

The Hungarian E-commerce Act regulates a wider set of services and also considers location tool service providers (i.e. search engine providers) and application suppliers intermediary service providers.[8] The reason behind considering application suppliers intermediaries lies in the new developments of the communications sector whereby internet-technology based services gain more emphasis. In today's chain of communication mere conduits are becoming mere infrastructure providers, because they do not have control over the transmitted information. Application service providers provide electronic data transfer services which are similar in nature to traditional electronic communications services (such as instant messaging applications). Search engine providers are also considered intermediary service providers by the Hungarian E-commerce Act due to their special role in the chain of online information flow. There providers doesn't host nor provide access to electronic data, but they have a closer connection to it than mere conduits. Search engine providers facilitate the easy findability of information online and in order to do this effectively they use algorithms to – among others – aggregate and rank information on the web.

There should be noted that there is a commonly used term both in the Hungarian and the European legal terminology: 'electronic communications services provider'. The rules of the Hungarian Act

[6] 2nd WORKING DOCUMENT(B) on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. (2018/0108 (COD)) -Scope of application and relation with other instruments. Committee on Civil Liberties, Justice and Home Affairs. Rapporteur: Birgit Sippel.
[7] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market OJ L 178, 17.7.2000, p. 1–16.
[8] Act CVIII of 2001 on Electronic Commerce and on Information Society Services Section 2. l)

XC. of 2017. on the Code of Criminal Procedure (hereinafter: Code of Criminal Procedure) mention these providers as the subjects of obligations. According to the interpretative provisions of the Hungarian Act C. of 2003. on Electronic Communications (hereinafter the Electronic Communications Act) the main element of the definition of electronic communication service provider is that it consists wholly or mainly in the conveyance and, where applicable, switching or routing of signals. [9] There is an overlap between intermediary service providers and electronic communication service providers: those intermediaries that are mere conduits and providers of network access services (the internet service providers) are electronic communication service providers as well.

The Hungarian legal system does not trust the providers with the decision on the amount of their involvement in the work of the investigative authorities, since both the Criminal Procedure Act and the Electronic Communications Act are very specific in terms of the obligations of the providers during the investigative process. However, there are no common rules for all the intermediary service providers: each type of provider has their own set of obligations based on their position and role in the process of online communication. The following section of the study aims to give a short overview of the obligations that intermediary service providers have to undertake.

3. Obligations of intermediary service providers in relation to the criminal procedure

3.1. Request for information, data retention

The Hungarian Code of Criminal Procedure states that the supply or transmission of information, data or documents can be requested from any public body, business organisation, foundation, public endowment and public organisation.[10] Therefore, upon receiving such a request, intermediary service providers and the other electronic communications service providers must provide the requesting organization with the specified data. Some investigative authorities can only request data supply from electronic communications service providers with a warrant issued by public prosecutor's office[11], except when issuing the warrant would result in a delay that is seriously detrimental to achieving the goals of the investigation. If the requested organization fails to fulfil the request within the prescribed deadline, or unlawfully refuses to fulfil the request, a disciplinary penalty may be imposed and other coercive measures may be ordered.

Despite their obligations to provide information to investigative authorities in criminal proceedings, most of the providers do not have a general obligation to store data related to their users. Even if a provider does have an obligation to store data, it does not include all kinds of data handled by the provider only certain types of it, furthermore the law sets out a time limit after which stored data should be deleted. The Hungarian Electronic Communications Act that is based on the European data retention directive[12] regulates only the data retention obligation of the electronic communication service providers and specifies the categories of data that are affected by this

[9] Electronic Communications Act Section 188. 14.
[10] Code of Criminal Procedure Section 261. (1)
[11] Namely the internal crime prevention department and the intelligence department of the police and other investigative authorities furthermore the counterterrorism department of the police.
[12] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC OJ L 105, 13.4.2006, p. 54–63.

obligation[13]. It has to be noted that the European equivalent of this provision had a rather controversial history, because Data Retention Directive[14] was invalidated by the CJEU in the judgement in Digital Rights Ireland and Seitlinger cases[15]. The Court stipulated that the main reason for the invalidity of this piece of legislation was the data retention obligation of this scale interferes with the right of privacy and the right to the protection of personal data in such a particularly serious way, which is not in compliance with necessity and proportionality requirements. The arguments of the CJEU focused on the fact, that the authorities were able to request data retention anytime in cases of serious crimes, which however are not defined properly, and in relation to all users and devices. Although Directive was invalidated, the provisions of the Hungarian Electronic Communications Act were not modified substantially; the Hungarian rules still oblige the providers to retain a wide range of data. Besides this, the Hungarian provisions have always ignored one of the guarantees of the Directive and haven't limited the objective of the data retention obligation to fight against serious crimes. The Electronic Communications Act states that the main goal of the data retention obligation is to ensure the discharge of the legally defined respective duties of those bodies that are authorized to request data.[16]

The rest of the intermediary service providers, the hosting service providers, search engine providers and caching providers doesn't have a general data retention obligation, despite the fact that they could contribute to the success of the investigations in many cases. The Hungarian E-commerce Act was modified in 2016, and according to the explanatory memorandum to the bill, the goal of the revision was to create a basis for the data retention and cooperation obligation of all the providers regulated by the Act. Contrary to this statement, the revised Act only contains one provision, which sets out a data retention obligation for application service providers only and under very special circumstances. Those application suppliers who provide information society services featuring encrypted communication between users, shall safeguard and disclose metadata when so requested.[17]

Despite the fact that there is no general data retention obligation that applies to all intermediary service providers the court, the prosecutor and the investigating authority may order the retention of specific electronic data on an individual basis. The obliged provider may be the holder, the processor, controller of the data in question and since all intermediaries are able to perform these operations on data, any of them could be the subject of this obligation. The provider on which this retention obligation was imposed should invariably retain the data in question and should ensure its secure hosting, prevent any activity that would result in its change, deletion, destruction, transfer and prevent the unlawful creation of copies and unlawful access to it.[18]

3.2. Cooperation in covert information gathering and for the use of covert means

The new Code of Criminal Procedure of Hungary which has entered into force in 2018 stipulates that with a judicial permit the information systems may be covertly surveilled and/or signals sent

[13] Section 159/A (1)
[14] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC OJ L 105, 13.4.2006, p. 54–63.
[15] C‑ 293/12 and C‑ 594/12. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.
[16] Section 159/A (1)
[17] E-commerce Act. Section 3/B.
[18] Code of Criminal Procedure. 316.§ (1)-(4)

through electronic communication networks by electronic communication devices may be intercepted.[19] There is a difference between the surveillance of a system and the interception of communications. While surveillance of an information system means the examination of the whole system including static (stored) and dynamic data (communication), during the interception of communications only the network traffic is being examined. To conduct the former, access to the computer itself is needed, while network traffic interception can be conducted remotely with the cooperation of the internet service provider as well. In Hungary several organizations are authorized by sectoral laws to conduct covert information gathering and to use covert means: the act on public prosecutor's office[20], the act on police[21], the act on the National Tax and Customs Authority[22] and the act on national security[23] all give authorization to certain organizations. In order to enable the aforementioned agencies to perform these actions, the Electronic Communications Act requires electronic communications service providers to cooperate.[24] During the course of the cooperation the electronic communications services providers should provide the conditions for the application of the means and methods of acquisition of messages and communications and data transmitted through the network in respect of the equipment and premises used and operated by them.[25] Furthermore the providers shall set up an appropriate technical system that meets the requirements of the authorized organizations – in particular a basic monitoring subsystem – and shall bear all the costs of these systems[26]. There is a Government Decree 180/2004. which sets out the detailed rules of the cooperation between providers and organizations that are authorized to conduct covert information gathering and use concealed tools.[27] According to the decree, the service provider shall provide for the conditions of covert information gathering such as providing a restricted space for the placement of devices to be used, ensuring that there are competent employees present and establishing a 24/7 on-call duty system.

If there is a need to create more detailed rules for the order of cooperation, the organizations authorized for information gathering can initiate the conclusion of a memorandum of understanding with the electronic communication service provider. This memorandum of understanding is an atypical contract, whereby the providers are obliged to conclude the contract within 60 days from its initiation. According to the Hungarian Civil Code, an obligation to contract may be prescribed by any piece of legislation, when there is a public interest objective that justifies the use of such an instrument[28]. This obligation shall be imposed only in exceptional cases, because it limits the provider's freedom to enter into contracts. The detection and sanctioning of cybercrime however is a valid public interest objective, that can serve as a basis for the limitation of the providers freedom to enter into contracts. Such memorandums of understanding are widely used in Hungary: most of the electronic communication service providers has such a cooperation agreement with the Hungarian National Police Headquarters[29].

[19] Code of Criminal Procedure Section 232.
[20] Act CLXIII on the public prosecutor's office.
[21] Act XXXIV. of 1994. of the police.
[22] Act CXXII. of 2010 on the National Tax and Customs Authority.
[23] Act CXXV. of 1995 on national security services.
[24] Electronic Communications Act Section 92. (1)
[25] Electronic Communications Act Section 92. (4)
[26] Electronic Communications Act Section 92. (5)
[27] Government Decree 180/2004 (V.26.) on the order of cooperation between organizations performing the electronic communication tasks and organization authorized for secret data collection and secret information gathering
[28] Act V of 2013 on the Civil Code Section 6:71 [Statutory obligation to conclude a contract].
[29] See for example: http://www.police.hu/sites/default/files/ot_2_0.doc

Those application suppliers who provide information society services featuring encrypted communication between users, where the content of communications or the functions related to establishing communication channels are not exclusively implemented on the user's terminal equipment (end-to-end encryption), shall be required to disclose to the agency authorized to conduct covert investigations the contents of transmissions.[30] By this provision the Act allows for the interception of such communication which takes place by the use of applications that have similar functions as electronic communication service providers, such as instant messaging (Viber, Whatsapp), therefore it provides the authorized bodies with an instrument similar to traditional wiretapping.

3.3. Rendering electronic data temporarily or permanently inaccessible

There are three types of cybercrime according to the Convention on Cybercrime[31] which was ratified by Hungary in 2004. The first group of cybercrimes consist of the offences against the confidentiality, integrity and availability of computer data and systems. The subject of these crimes is the information system and the tool of the commission of the act is usually the information system as well. The second group consists of the 'computer related' offences, where the subject and the tool are also the information system but the act is committed with a fraudulent intent to either produce inauthentic data to be considered or acted upon for legal purposes as if it were authentic, or to gain economic benefit.[32] The third and broadest category of cybercrime is the category of content related offences (child pornography and copyright infringements).The Hungarian legal system recognizes more offences as content related crimes: libel and slander are criminalized in Hungary and constitute a content-related cybercrime when committed by the use of the internet. In Hungary there are many methods of making providers remove illegal content, but these measures are scattered throughout the legal system and doesn't form a coherent system. The Code of Criminal Procedure provides a two-tier solution for rendering electronic data temporarily inaccessible:[33]

- in the case of offences where there is place for public prosecution, the hosting service providers and those intermediary providers which offer hosting services as well, may be obliged to temporarily remove allegedly unlawful data[34].

- In the case of serious offences such as drug trafficking, child pornography, offences against the state and terrorist offences, investigative authorities may order internet service providers to render electronic data permanently inaccessible if hosting service provider mentioned in the previous point failed to comply with its obligation the remove the data in question[35]. Rendering electronic data temporarily inaccessible may be ordered if the hosting service provider is established abroad and requests for mutual assistance didn't bring a result. In this case the obliged electronic communication service provider shall fulfill the request in compliance with the procedure and technical specification prescribed by the National Media and Infocommunications Authority.

It has to be noted that there is a difference between the two instruments. In the first case the data itself is removed from the server on which it is hosted. In the second case it isn't, merely access is

[30] E-commerce Act Section. 3/B.
[31] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[32] Convention on Cybercrime, Title 2 – Computer-related offences.
[33] Code of Criminal Procedure Section 335.
[34] Code of Criminal Procedure Section 336.
[35] Code of Criminal Procedure Section 337.

prevented through technical blocking solutions (for example by blocking the URL or the IP address) and it remains available to subscribers of other countries or subscribers who use VPN services or web browsers routing the information through proxy servers (such as TOR). Both measures are temporary and can only last until the final judgement in the case is reached by the court. If the court rules that the information is indeed unlawful, rendering the data permanently inaccessible must be ordered pursuant to the provisions of the Hungarian Penal Code.[36] But if the court finds that the electronic data is not unlawful, the court orders the restoration of the data or the unblocking access to the data.

Besides these measures there is one supplementary provision in the Code of Criminal Procedure, which is used to notify media content provider, the hosting service provider and other intermediary service provider about allegedly unlawful content before they receive an official order from the investigative authorities.[37] Pursuant to the notification the providers have the right to evaluate the information in question and voluntarily remove it, if they find it unlawful. The aim of this provision is to facilitate the swift removal of clearly unlawful information (such as child pornography) because if the provider acts on its own volition there is no need to wait for the court's permission to issue an order to remove the data, which can take a long time. There is another less manifest aim of this provision: to give rise to the liability of the providers for third party information. Despite the fact that the act stresses that the removal based on such a notification is voluntary, the provider may be held liable under the E-commerce Act as a consequence of its ignorance or its misjudgment of the unlawful nature of the information. The next chapter of this paper will examine the liability framework of intermediary service providers in Hungary in detail, but here we should note that the E-commerce Act – similarly to the E-commerce Directive – stipulates that the hosting provider shall only be exempted from liability for third party information if it doesn't have knowledge of the unlawful nature thereof. After the reception of the investigative authority's notification the provider can no longer successfully argue that it didn't have knowledge of the allegedly unlawful third-party information hosted in or transmitted through its service, since it was brought to its knowledge directly and in order to make the decision not to remove it, the provider had to make its own assessment. It is quite clear that the removal of the information based on the notification is only namely voluntary, because the provider has to take into account that not removing the information, may give rise to its own liability and possibly its sanctioning, which is not a very attractive option.

4. The instruments to remove unlawful content outside the system of criminal procedure

4.1. Notice and takedown procedure

There are other methods to remove unlawful content from the network that fall outside the scope of criminal proceedings. The E-commerce Act only provides for the exemption of the hosting provider and the search engine provider from liability if the provider upon obtaining knowledge of illegal activity in connection with the information acts expeditiously to remove or to disable access to the information. This obligation applies regardless of the source of the information, so stakeholder notification or complaints are both suitable to invoke liability. The Hungarian E-commerce Act contains more detailed rules on intermediary liability than the E-commerce Directive and sets up a notice-and-takedown procedure. The Hungarian notice-and-takedown procedure can only be used in

[36] Penal Code Section 77.
[37] Code of Criminal Procedure Section 338.

two instances: in the case of copyright infringements and in the case of infringement of minor's personality rights. The procedure starts with the notification of the intermediary service provider in a private document representing conclusive evidence or in an authentic instrument. Pursuant to the reception of the notification the provider has 12 hours to take the measures necessary for the removal of the information indicated in the notification, or for the disabling of access to it.[38] The mere conduits and the ISPs do not have similar obligations, so if these providers obtain knowledge of illegal activities in connection with their networks, they do not have to take any measures in order to terminate it. Usually due to network security reasons the providers do put an end unlawful activities. The largest Hungarian ISP-s all include provisions into their end-user contracts which allow for the termination of the service if they notice any unlawful communications.

4.2. Administrative action against illegal media content

If an infringement occurs in services that are to be regarded as media services or online press products the Hungarian Media Council can also order intermediary service providers to disable access to the service in question.[39] The new Audiovisual Media Services Directive (hereinafter the AVMSD)[40] stipulates that video-sharing platforms providers have to take certain measures in order to protect the audience from content the dissemination of which constitutes an offence under EU law[41]. As video-sharing platforms are hosting service providers, we have to highlight that one of these obligations shall be the introduction of complaint procedures, where the provider has to assess the unlawfulness of the content and remove it if it might indeed constitute and offence. Although the AVMSD itself doesn't set out a specific obligation to take down presumably unlawful content, gaining knowledge of such content through user's complaints also serves as a basis for provider's liability.

4.3. Internet Hotline

Hotlines are commonly existing organizations throughout Europe, with aim to facilitate the fast removal of illegal content. The Internet Hotline[42] operates in Hungary since 2015 and it is a part of the INHOPE network.[43] Users can make complaints in the following nine categories: content made accessible without permission, online harassment, paedophile content, racist / hateful content, violent content, data phishing sites, content infected with viruses, spyware or worms, content promoting drug use, content inciting acts of terrorism, promoting or contributing to terrorism, other content that may be harmful for minors. When the associates of the Hotline find, that the referred content is illegal, they ask the content provider (who made the content available) to delete it. If the content provider doesn't comply, the Hotline asks the operator of the server on which the content is hosted to remove it. The Hotline – despite that it is a useful tool – is only a legal aid service, its decisions and orders are not binding to the providers.

[38] E-commerce Act Section 13. (4)
[39] Media Act Section 188. (2)
[40] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities OJ L 303, 28.11.2018, p. 69–92.
[41] AVMSD Article 28b. 1. (C)
[42] http://english.nmhh.hu/internethotline/
[43] http://www.inhope.org/gns/home.aspx

4.4. Self-regulation and corporate social responsibility

Frosio notes that governments try to coerce online intermediaries into implementing policy strategies such as graduated response, monitoring and filtering obligations through self-regulation and voluntary measures. [3] Some providers have adopted measures to tackle the issue of unlawful content online, for example, big providers such as Google and Facebook have detailed community guidelines to regulate user's behaviour. Recently the notion of corporate social responsibility has gained popularity pursuant to which providers take certain actions to protect users and fundamental values online. At this point we should echo Laidlaw's concern [7] who thinks that from a human rights perspective the ultimate question is, whether the CSR frameworks are sufficient to provide the standards and compliance mechanisms needed to protect and respect fundamental rights such as freedom of expression. Some scholars argue that the responsibility of intermediaries shall be examined from a moral rather than a legal point of view, yet scientific literature lack the description of the ethical framework which define service providers' responsibility [9].This phenomenon also exists in Hungary, because the key players of the industry are global companies who operate on the Central-Eastern-European markets. András Koltay draws attention to a problem caused by that these providers have established a 'pseudo legal system', namely that regulation of democratic publicity gets outsourced and the procedural guarantees that stem from the principle of the rule of law doesn't exist in these systems. [5]

5. The liability of intermediary service providers in Hungary

5.1. Intermediary liability in general

The existence and extent of intermediary liability is a much-debated area of legal literature. The first ideas on intermediary liability – especially on the liability of the ISPs – have emerged in the United States, where the notion of intermediary immunity was codified by the Communications Decency Act in 1996. The European Union adopted a regime of limited liability, without the introduction of a notice and takedown regime. The rules of the E-commerce Act constitute a horizontal framework for liability, which means that they are to be applied on all legal areas, therefore when conditions are met, the provider is exempted from both criminal and civil liability. The basis of the Hungarian liability framework is that service providers shall be liable for any unlawful information they have made available.[44] In some cases however providers can be held liable for third party information as well. Such as the liability of ISP's, the liability of intermediary service providers can be described as secondary liability, tough there are ongoing debates about the interpretation of this term in different legal systems. [1] As László Dornfeld notes there are pragmatic reasons for holding providers liable: contrary to the users who are unknown and unidentifiable, the service providers are relatively easy to find and pursue. [2] The E-commerce Directive and the Hungarian E-commerce Act both list the conditions that should be met in order to be exempted from liability for third party content. Liability itself is however not homogenous in nature, the conditions that allow for exculpation are different and the differentiation is based on the activities of the provider. Ákos Kőhidi highlights that in the case of mere conduits and caching the facts that justify limited liability are objective in nature, while in the case of hosting services and search engines there is a subjective element: becoming aware of the unlawful information.[6] Mere conduits are not liable for the information transmitted, on condition that they do not initiate the transmission; does not select the receiver of the transmission; and does not select or modify the

[44] E-commerce Act Section 7. (1)

information contained in the transmission.[45] The E-commerce Act sets out the same conditions for the exemption of application service providers.[46] Caching providers are not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that they:

- do not modify the information;
- comply with conditions on access to the information;
- comply with rules regarding the updating of the information, specified in a manner widely recognized and used by industry;
- do not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and
- act expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.[47]

Hosting service providers are not liable for the information stored at the request of a recipient of the service, on condition that they do not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.[48] According to the E-commerce Act, the same conditions apply for the exemption of search engine providers as well.[49]

The Hungarian law goes beyond the provisions of the Directive and contains additional rules that are to be applied in the case of copyright infringement and for the infringement of minor's personality rights. These additional rules introduce the Hungarian notice and takedown procedure which was elaborated in detail by the previous section of this study.

5.2. Criminal liability of intermediary service providers

The criminal liability regime that is to be applied to intermediary service providers complements the general liability regime set out by the Hungarian E-commerce Act. Only that perpetrator can be the subject of criminal liability. According the Hungarian Penal Code 'perpetrator' means the principal, the covert offender and the coactor, as well as the abettor and the aider (the accomplices).[50] Based on this, intermediary service providers are unlikely to be carry out the acts described by the Criminal Code, because they are in most cases legitimate economic services without the intention to carry out criminal activities. They may be accomplices by knowingly and by voluntarily aiding the

[45] E-Commerce Directive Article 12.
[46] E-commerce Act Section 8.
[47] E-Commerce Directive Article 13.
[48] E-Commerce Directive Article 14.
[49] E-commerce Act Section 11.
[50] Criminal Code Section 12.

commission of a crime. Aid can be physical, for example by making the infrastructure available for criminal use and psychological for example by encouraging the offenders to use their infrastructure for their purposes. Both physical and psychological aid can be realized in a form of a deliberate act or an omission and for the purposes of this study the latter is more interesting. The previous part of this study gave a short introduction to those measures that providers can be ordered to do to aid criminal investigations. Providers can opt for non-compliance in which case they are in failure to act, despite that they had a legally imposed duty to do so. In this case an omission can give rise to criminal liability.

5.3. Civil liability for criminal conduct

The most common debates around intermediaries concern the civil liability for the loss or harm caused by third party content. In Hungary the Code of Criminal Procedure allows for pursuing civil law claims for compensation in criminal procedures. The general liability framework of the E-commerce Act also applies in these situations, but if the conditions to be exempted from liability are not met, providers can be held liable for damages. In American legal theory the notion of intermediary immunity starts to shift towards intermediary liability. Lichtman and Posner for example note that ISP's are in a perfect position to tackle the distribution of malware, therefore they should have a duty to prevent the dissemination of such information. The authors set up a 4-tier argument to show when would it be appropriate to hold ISP's liable for unlawful third-party information. Holding intermediary service providers liable can be a viable option if the individuals who commit the act are hard to identify, the affected parties can allocate liability efficiently through contractual design, the ISP can detect, deter or otherwise influence bad acts in question and where providers can internalize negative externalities. [8]

6. Conclusions

As shown in the first section of this study intermediary service providers can aid criminal investigations in various ways: with simple information sharing and by blocking websites alike. Most of the activities of these providers however are not voluntary, they are based on legally set out obligations. Non-compliance, may give rise to the provider's criminal and civil liability, but liability for third party information is limited, because if certain conditions are met, providers may be exempted. By abiding the law and fulfilling their mandatory obligations during criminal investigations the providers may also avoid being held liable. However this approach hinders their willingness to introduce voluntary measures to combat these crimes. Originating from the United States a new approach is emerging, which stipulates that providers should be held liable for third party information, because they have a responsibility, and the means to prevent cybercrime. The theories of moral responsibility and platform self-regulation have started to appear in Europe as well, but further research is needed to examine the possible effects of the extension of intermediary liability and also to clarify the connection between liability and responsibility in continental legal theory.

7. References

[1] DINWOODIE, G. B., A Comparative Analysis of the Secondary Liability of Online Service Providers. In: Dinwoodie, Graeme B. (ed.): Secondary Liability of Internet Service Providers, Springer, 2017. p. 2.

[2] DORNFELD, L., A közvetítő szolgáltatók felelőssége az internetes tartalmakért KRIMINOLÓGIAI KÖZLEMÉNYEK 78 pp. 101-117, p. 17 (2018).

[3] FROSIO, G. F., Why keep a dog and bark yourself? From intermediary liability to responsibility International Journal of Law and Information Technology, Volume 26, Issue 1, 1 March 2018, p. 1–33.

[4] KLEIN, T., (szerk.), Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről Budapest, Magyarország, Médiatudományi Intézet (2018) , p. 12.

[5] KOLTAY, A., Az újmédia kapuőreinek hatása a médiaszabályozásra. In: Gellén Klára (szerk.): Jog, innováció, versenyképesség. Budapest, Wolters Kluwer, 2017, p. 99-124.

[6] KŐHIDI, Á., A jogsértő internetes tartalommal szembeni jogi eszközrendszer In: Koltay, András; Török, Bernát (szerk.) Sajtószabadság és médiajog a 21. század elején 3 Budapest, Magyarország : CompLex Wolters Kluwer, (2016) pp. 375-402. p. 27.

[7] LAIDLAW, E. B., Internet Gatekeepers, Human Rights and Corporate Social Responsibilities. A thesis submitted to the Law Department of the London School of Economics and Political Science For the degree of Doctor of Philosophy. 2012. p. 111.

[8] LICHTMAN, D. G. and POSNER, E., Holding Internet Service Providers Accountable (John M. Olin Program in Law and Economics Working Paper No. 217, 2004).

[9] TADDEO, M. and FLORIDI, L., The Moral Responsibilities of Online Service Providers. In: Taddeo, Mariarosaria, Floridi, Luciano (Eds.): The Responsibilities of Online Service Providers, Springer, 2017. p. 14.