Eötvös Loránd University

Faculty of Law, Doctoral School of Law and Political Sciences
Head of the Doctoral School: Prof. Dr. István Kukorelli, DSc.

The role and responsibility of internet intermediary service providers in tackling information technology crime

PhD. dissertation

THESES

Written by: Kinga Sorbán

Doctoral supervisor

Prof. Dr. Géza Finszter, professor emeritus, DSc.

Budapest

2021.

Aim of the dissertation and relevance of the chosen topic

The internet as the global network connecting computers is a crucial part of our everyday lives, since it became commercialized in the 1990's. In our present days, our private lives and work are both unimaginable without the internet and connected devices. It may not be an exaggeration to state the internet has opened up the world: new dimensions of entertainment, information gathering and informing the public were brought about by the system, connecting almost every point of the globe 24/7 offering real-time connection. Besides its numerous advantages the world wide web has opened a path for evolved criminality.

Old crimes appeared in new forms, such as harassment, and it soon became evident that some of the new activities has to be penalized to protect society (such as crimes against information systems and data). Online criminality creates constantly appearing challenges for lawmakers and practitioners alike. András Koltay draws attention to that some law infringements online (such as the dissemination of hate speech) are regulated by laws that were not specifically designed to tackle the challenges of the online sphere. Lawyers thus aim to interpret law infringing conduct occurring on the internet in a way to be able to squeeze them into the existing legal frameworks, given that it is possible to do so. Existing rules however aren't applicable to every conduct realized in the online environment as freshly developed activities sometimes doesn't match the paragraphs of the law in effect (see for example the phenomena called revenge porn by laymen terms which can be committed by the dissemination of pornographic material without the consent of the person(s) depicted). Due to the fundamental principle of *nullum crimen sine lege*, the use of an analogy in criminal law is out of the question, thus practitioners can not construct new norms by selecting and merging relevant phrases of different sections of the Criminal Code. The dynamically developing technology and ever-changing user behaviour call for the constant development and renewal of legislation, which poses a rather serious legal policy dilemma. If the law changes fast to keep up the pace with new conditions, it may become so pliable that it may endanger the stability of the legal system, which is not a desirable outcome. If however it fails to give a timely regulatory response to new phenomena it may fail to fulfil its obligation to protect the individual users and society as a whole.

A similar dilemma has been phrased before in relation to technology regulation in 1980. The Collingridge-dilemma describes the following regulatory issue: the effects of new technology cannot be measured properly until its fully developed and applied widely, yet when the technology is already widespread it is difficult to tackle problems that arise in relation to its application by regulation and influence changes. [1] Probably this dilemma will never be resolved by legislation due to another dilemma: the so-called pacing problem. The pacing problem described by Larry Downes in 2009 means that while technology changes in an exponential rate, societal, economic and legal systems only change in a limited pace. [2] Adopting regulation prematurely to fast changing behaviour may not yield the expected results because by the time the new rule gets adopted and becomes applicable to the conduct that was the subject of the legislation may have changed in a way that it is not relevant anymore or is committed differently, rendering the newly adopted rule outdated. In the early years of the internet the commission of the so-called dial-up frauds and machine time theft were common and popular, but with the spread of broadband internet connection vanished completely.

In the light of these dilemmas it is of paramount importance to define when it is necessary to sanction new harmful conduct by creating new legislative instruments and when is it enough to adapt already existing rules to tackle new situations. One of the aims of this dissertation is to draw attention to the moderns deviancies of the virtual world, to point out those acts that should be criminalized and to highlight those new phenomena which can be handled effectively using the criminal laws in force.

Szilvia Dobrocsi and Andrea Domokos sum up these issues by phrasing the question whether there is a need for a „digital Criminal Code"? [3]

It must be noted that fresh pieces of legislation do not arrive into a vacuum; as the current rules within the criminal code do not exist in a sterile environment either: the norms of other legal

---

[1] David Collingridge: Social Control of Technology. Continuum International Publishing Group Ltd. 1982.

[2] Larry Downes: The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age, Basic Books, 2009.

[3] Dobrocsi Szilvia – Domokos Andrea: Kiberbűnözés. In: Homicskó, Árpád Olivér (szerk.) Egyes modern technológiák etikai, jogi és szabályozási kihívásai. Budapest, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar, (2018) pp. 49-74., 50.o.

field have relevance and affect the norms of substantive and procedural criminal law. Criminal law as Decision no. 30/1992. (V. 26) of the Constitutional Court puts it is „the sanctioning cornerstone of the overall legal system"[4] or in other words it is the ultima ratio solution of the liability system. Whether to criminalize new and harmful activities must be assessed using rigid standards, with due consideration of constitutional objectives and values at all times. Prior to deciding when and how to sanction newly emerged internet-based conduct by the tools of the criminal law, one must carefully evaluate the applicability of sanctions set out by other relevant legal fields. In the case of dissemination content or speech online the framework of protecting personality rights of the civil law shall be considered.

As the criminalization of disseminating content always invokes freedom of speech issues one must always consider how certain restrictive measures and criminalization of the dissemination of certain content interfere with this fundamental right. There may be some instances where protecting the right to freedom of speech serves the public interest more than criminalizing speech that is harmful to individuals. The second goal of the dissertation is to map when and to what extent shall the right to the freedom of speech restricted in relation to new hand harmful online conduct using the tools of criminal law.

There are some forms of speech that are already criminalized by the Hungarian Criminal Code: these instances of speech restrictions were analysed by the Constitutional Court of Hungary, the Court of Justice of the European Union and the European Court of Human Rights alike. The conclusions drawn by these judicial bodies serve as examples that guide the assessment of restricting the dissemination of new forms of harmful online speech with the tools of criminal law.

One must not fail to take into account the significance of private regulation, because some internet intermediary service providers (such as video-sharing platforms) apply restrictive measures by themselves and ban the dissemination of some forms of speech. Prohibiting the dissemination of content in the terms of services of internet intermediaries is not necessarily aligned with the types of content which's dissemination constitutes a criminal offence resulting in a dissonance between different levels of protection. Content forms that are prohibited by service providers are not always law infringing materials (see for example the practice of Facebook and YouTube which ban all forms of nudity from their platforms), yet these prohibitions influence user behaviour similarly to the provisions of criminal law. On the other hand several content types are not prohibited by platforms even when their dissemination constitutes a criminal offence in certain jurisdictions. The service providers often argue with the protection of freedom of speech. One of the hottest topics of current regulatory debates is whether platforms are capable to put pressure on national sovereign legislators and influence national laws to criminalize some activities. The thesis will compare Hungarian and EU norms with the frameworks set up by big intermediary service providers in order to map notable differences and grey zones.

The main objective of criminal law is to protect society, general and special prevention. The criminal procedure is what contributes to the reaching these objectives by prosecuting individual offenders. Prosecution is however challenging when it comes to online conducts. Online communication can be anonymous and encrypted which makes identifying the offenders and discovering the acts hard. Internet criminality is a global phenomenon, which is independent of national borders; the lack of territoriality can obstruct the success of prosecution. The EU and the Council of Europe aimed to approximate national criminal law provisions – the Cybercrime Convention for one draws up a list of cybercrimes which includes the majority of internet-facilitated offences – but due to the differing legal traditions and culture of the signatories there are many differences. These differences are more prominent between some

[4] point 4. https://hunconcourt.hu/uploads/sites/3/2017/11/en_0030_1992.pdf

EU Member states and third countries such as the USA. The USA protects freedom of speech more than the majority of European, including the Hungarian, legal systems. For example libel / slander are not criminal offences, and holocaust denying speech is often allowed on social media platforms. This differences pose challenges to the international enforcement of national norms: imagine the situation where a Hungarian Facebook user deems a comment under his post deeply offensive, yet it is considered acceptable as a form of free speech for an American user who will not be held liable. These obstacles not only affect the application of procedural provisions but also the substantial provisions which are being enforced, so one might eventually question whether it is worthwhile to keep national norms that are unenforceable in the online environment. This is a really pressing issue in the case of those activities that's decriminalization is already the subject of discussion in the Hungarian legal thinking regardless of the ongoing debates about online enforcement. An example is criminal libel which's decriminalization was urged by András Sajó in 2005. [5]

The inverse of this situation is not unimaginable and may pose unique challenges as well, when regardless of an obligation set by international law, Hungarian law is forced to implement the regulatory method of an other country. As the market leading companies of the online communication sector are based in the Silicon-valley, the regulatory influence of the USA may be an example, which affects many countries' legal system indirectly through regulation of US-based internet intermediaries. Such rules will be foreign bodies in the Hungarian legal system as some of the underlying legal notions can be insterted only partly or cannot be inserted at all into the dogmatical system developed over a long period of time.

Besides the differing regulatory environment, enforcement may have other obstacles. Information-technology crimes are crimes that can be tackled by persons with specific expertise, requires cross-border cooperation and enormous resources, which national organizations usually aren't able to provide, but market players are. Internet-based crimes cannot be committed without using one or more internet intermediary service providers; the functioning of these providers in fact interweaves the commission of these offences or the service itself is the medium in which the unlawful action takes place. Hackers entering IT systems need internet connection which is provided by mere conduits (commonly known as internet service providers, ISPs). The situation is more complex in the case of offences realized by the disseminating some kind of content or speech, where the typical „place" of commission is the platform of a social media service provider (for example Facebook) or a video-sharing platforms service provider (for example YouTube), where the hosting providers have a great role in recognizing the offence and mitigating harms by removing certain content. On the basis of this recognition the thesis is going to elaborate how and where internet intermediaries can intervene to tackle offences. Recognising the special position of these providers, many jurisdictions require their contribution to the investigative process and to the enforcement of coercive measures.

Act XC. of 2017 on Criminal Procedure puts several obligations on internet intermediary service providers. Mere conduits (ISPs) have to contribute to the application of the use od covert information gathering methods such as online wiretapping or rendering electronically stored data temporarily of definitely inaccessible (blocking websites), while hosting service providers may be obliged to remove certain content and giving out law enforcement authorities the IP address of the law infringing user. There are several criminal acts committed in the online sphere which could not be tackled without involving certain intermediary service providers, thus criminal justice systems are not able to avoid relying on the aforementioned industry actors. The position of these providers within the criminal justice system is however not clear as the Act on Criminal Procedure does not define a specific position for intermediary service

[5] Sajó András: Becsületvédelem és büntetőjog - megjegyzések a becsületsértés dekriminalizálásáról, Budapest: Büntetőjogi kodifikáció, 2005/1. szám: 3-6.

providers. Successful cooperation however assumes a clearly and concisely regulated relationship between state actors and private entities on national and on international levels alike. Even tough there are a handful of procedural acts where law enforcement authorities rely on the help of market players, these companies are not the same level las authorities but they are in a subordinate role in which state is the legislator and the provider is the subject of legislation. Being a subject of regulation is specifically interesting in those situations where the market player in question has clear dominance: for example due to the fact that is possesses data that is indispensable for an investigation or where the provider is under an other country's jurisdiction. The dissertation's author considers her main task to map the relationship of state actors and service providers contributing to the success of investigations. Not only the role and obligation of the intermediary service providers remain undefined, the scope of these providers' liability in an open question too. In the wake of the new millennium when online communication became mass-communication, legal systems provided immunity to providers to shield them form liability for law-infringing content stored or shared by third parties.
In this context liability is not necessarily criminal liability but liability overarching different legal areas. Such general immunity is provided by Section 230 of the Communications Decency Act (CDA) in the USA. The EU envisaged a similar system of limited liability by adopting the 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 (E-commerce Directive).
The paradigm according to which platforms have limited liability for data present in their services seems to shift in our present days as some providers (for example social media service providers) started to actively participate in the communicative process – see for example the tension between former US president Donald Trump and Twitter. In conclusion there are some providers which may in some cases be held liable for content on, or information transmitted through their services, while they are expected to act contributors to the procedure or partners of law enforcement authorities. It is easy to realise that there may be cases where the best interest of the provider is not to cooperate with law enforcement authority but aid the ones committing the offenses while trying to avoid liability. The liability regime applicable to the providers thus has to be redefined in a way in which the providers' best interest would always be to cooperate with law enforcement authorities without having to fear the consequences of aiding the investigative process.

The structure of the thesis

The current thesis includes 9 chapters. The first chapter aims to lay down the foundations by defining key terms which are needed for several reasons. First, information technology crimes are special as it is impossible to discuss them by the utilization of traditional legal terminology. In order to convey the seriousness of the issues to the readers and elaborate on the background of legislative measures regulating the area, the basics of information technology has to be discussed as well. Second, due to the dissertation strongly relies on international regulatory trends one can not ignore the fact that the terms used to describe information technology crimes and related phenomena are not unified. Even the term information technology crime is an umbrella term used in many context, furthermore there are several other term to describe the same – or almost the same – set of offences (such as computer crime, high-tech crime, cybercrime etc.). Third, the regulation of technology and service providers has called for the development of several technology-infused legal term, applied by also by the Hungarian legal system.

A separate chapter gives an overview of information technology crime in an international context. The chapter discusses the history of computer and information-technology related criminality, illustrating the dynamics of development, emphasizing how fast technology changes. The legislative sources of information technology crime are discussed by a separate section of this chapter. As criminality involving computers appears in many EU and international legal instruments the relevant international laws are discussed in detail. As the majority of tech-companies addressed by the thesis are originating from the USA one must not underestimate the effects of US law to influence the actions of these companies (for example when it comes to their perception of freedom of speech issues), thus the law of the USA will be discussed in detail. This dissertation has a separate chapter (chapter IV.) on the Hungarian regulation of information technology crimes, describing the relevant elements of substantial criminal law in detail, drawing attention to service providers' practice to tackle conducts criminalized in Hungary and pointing out the problems that emerge. Chapter V. was reserved for those acts that are on the verge of being regulated by criminal law: these are activities that are not yet criminalized in Hungary or activities in which's case it is not clear which criminal provision should be applied (if any at all).

Chapter VI. aims to introduce the social context of information technology related criminality. The aim of the chapter it to draw attention to the fact that IT crime is not a marginal problem and does not only affect a narrow slice of society. Statistical data shows that the volume of information technology crime is not negligible even despite the fact we only have limited amount of information, which doesn't show the full scale of the problems. This part aims to lay the foundation of the following thesis: state intervention to regulate internet intermediaries is necessary for two reasons. One reason is that user literacy regarding information technology crime is low, which means that citizens are not able to protect themselves effectively in the online sphere, so the significance of state-pursued general prevention is high. The other reason why state intervention is necessary is that there is an unequal relationship between the users and the platforms; platform as the parties with stronger positions are not always capable and willing to address harms reported by the users, resulting in a strong need for state oversight.

The next major chapter (chapter VII.) evaluates the actions of platforms from the perspective of the criminal procedure, highlighting the obligatory and opportunistic measures platforms undertake, drawing attention to those contradiction that lie between platforms' obligations and liability for third party actions.

Pursuant to the detailed analysis of these issues the dissertation discusses those regulatory endeavours that are beyond the legislative acts in force and which are quite common in our present regulatory ecosystem (chapter VIII.). The private regulation applied by internet intermediaries, self- and co-regulatory measures not only constitute a method of enforcing existing legal acts but also a method of creating new rules and setting up new procedures through which providers do policing within their service. This chapter also includes the analysis of how state may be able to tackles challenges posed by providers' private regulation.

The concluding chapter of the thesis aims to summarize the former chapters and argues that a complete *de lege ferenda* proposal cannot be created at this point. The diverse role of intermediaries in regulation, enforcement and criminal procedure leads to the conclusion that traditional regulatory methods are not effective anymore – even tough they might not turn out to be complete failures especially in an environment which relies on services offered globally. Nevertheless the dissertation aims to offer some regulatory guidelines, drawing attention to main courses of action.

Methodology

The assessment of information technology crime, especially the evaluation of the role of internet intermediaries cannot be limited to the detailed analysis of one single area of law. As the regulatory and procedural dilemmas discusses within the dissertation are quite actual, adopting a multidisciplinary approach is of paramount importance, in which the assessment of substantive legal and procedural issues can be discussed as parts of a broader concept.

The dissertation is built on introducing British and US law from a comparative perspective and tacking stock of the notable pieces of international laws and the law of the European Union governing the area. The private regulation of the biggest online intermediaries is also introduced. The analysis of legal and extra-legal provisions are complemented by a theoretical analysis of the identified issues which is based on desk research concerning relevant scientific literature and conclusions drawn from existing case of Hungarian and international judicial bodies. As all of the issues that are discussed are rooted in the framework of fundamental rights, the author deemed it necessary to elaborate on the notable decisions of the Hungarian Constitutional Court, and the Curia of Hungary too.

Chapter VII. of the dissertation is built on the nationally representative survey conducted by the Institute of the Information Society (IIS) of the University of Public Service. IIS has ordered a nationally representative research in October 2019m which consisted of a survey with 1003 participants. Data obtained is representative for the adult population of Hungary in terms of age, gender, level of education, place of residence and region. The surveys were conducted through telephone interviews, done by MASMI Hungary market analysis company.

The publications in the field of research of the dissertation

1. Kinga Sorbán: The video-sharing platform paradox – Applicability of the new European rules in the intersection of globalisation and distinct Member State implementation. Communications Law, 25. (2020), 2. 89-100. o.

2. Kinga Sorbán: The role of Internet intermediaries in combatting cybercrime: obligations and liability. In Nemeslaki András – Alexander Prosser – Dona Scola – Szádeczky Tamás (szerk.): Central and Eastern European eDem and eGov Days 2019. Bécs, Austrian Computer Society, 2019. 19-31. o.

3. Sorbán Kinga: A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről. Belügyi Szemle 68. (2020) 10. 81-104. o.

4. Sorbán Kinga: A társadalmi tudatosság és az online közvetítő szolgáltatók szerepe az informatikai bűnözés elleni fellépésben. Iustum Aequum Salutare 16. (2020) 3.179-192. o.

5. Sorbán Kinga: A bűnügyi tudományok és az informatika – könyvismertetés. Belügyi Szemle, 67. (2019), 11. 99-103. o.

6. Sorbán Kinga: A videómegosztóplatform-paradoxon, avagy az új európai szabályok alkalmazhatósága a globalizáció és az eltérő tagállami implementáció keresztmetszetében. In Medias Res, 8. (2019), 2. 210-229. o.

7. Sorbán Kinga: Az internetes közvetítő szolgáltatók kettős szerepe a kiberbűncselekmények nyomozásában. Felelősség és kötelezettségek. In Medias Res, 8. (2019), 1. 84-101. o.

8. Sorbán Kinga: Vírusok és zombik a büntetőjogban: Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései. In Medias Res, 7. (2018), 2. 369-386. o.

9. Sorbán Kinga: A videomegosztó platformok európai szabályozásának aktuális kérdései. Médiakutató, 19. (2018), 1. 9-20. o.

10. Sorbán Kinga: A digitális bizonyíték a büntetőeljárásban. In Christián, László (szerk.): Rendészettudományi kutatások. Az NKE Rendészetelméleti Kutatóműhely tanulmánykötete. Budapest, Dialóg Campus, 2017. 129-136. o.

11. Sorbán Kinga: A digitális bizonyíték a büntetőeljárásban. Belügyi Szemle, 64. (2016), 11. 81-96. o.

12. Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés az Egyesült Államokban. Themis, 14. (2016), 1. 150-170. o.

13. Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés az Egyesült Királyságban. In Keresztes Gábor (szerk.): Tavaszi Szél 2015 / Spring Wind 2015 Konferenciakötet. I. kötet. Budapest–Eger, Doktoranduszok Országos Szövetsége, 2015. 339-355. o.

14. Sorbán Kinga: Informatikai bűncselekmények és nyomozásuk az Egyesült Királyságban. Belügyi Szemle, 63. (2015), 9. 48-68. o.

15. Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. Themis, 13. (2015), 1. 343-375. o.