SOFIA LOPES AGOSTINHO

ASSESSING ONLINE VIOLATIONS OF PRIVACY AND DATA PROTECTION THROUGH THE LENS OF CRIMINAL LAW

Dissertation to obtain a Master's Degree in Law,

in the specialty of Law & Technology

Supervisor:

Athina Sachoulidou, PhD

Assistant Professor, NOVA School of Law

September 2021

SOFIA LOPES AGOSTINHO

ASSESSING ONLINE VIOLATIONS OF PRIVACY AND DATA PROTECTION THROUGH THE LENS OF CRIMINAL LAW

Dissertation to obtain a Master's Degree in Law,

in the specialty of Law & Technology

Supervisor:

Athina Sachoulidou, PhD

Assistant Professor, NOVA School of Law

October 2021

Acknowledgements: To my family.

Way of citing: Chicago style (adapted).

The body of the thesis occupies a total of 175.903 (one hundred and seventy-five thousand nine hundred and three) characters including spaces and notes.

Anti-plagiarism statement

I hereby declare that the work I present is my own work and that all my citations are correctly acknowledged. I am aware that the use of unacknowledged extraneous materials and sources constitutes a serious ethical and disciplinary offence.

Sofia Lopes Agostinho

Abstract

In a context where the digital footprint becomes progressively “bigger” than the physical one, everyone accesses easily goods and services offered online. However, at the same time, new technological tools, such as smartphones, make users of the World Wide Web more vulnerable to intrusions in their privacy sphere.

Privacy violations, such as illegal interception, may compromise user’s safety both online and offline, exposing him or her to a great harm, often caused by a perpetrator that cannot be traced. Additionally, the lack of awareness of both the risks Internet users are facing and the protective measures they may take to address those risks increases their vulnerability significantly.

Against this backdrop, this thesis will examine the *status quo* of cybercrime – with a focus on those elements that distinguish it from the offline crime: the anonymity of the perpetrator, its global reach and scalability, the transnationality of cybercrime as well as the difficulties of addressing it by means of robust and immutable regulation.

Moreover, this thesis delves into the EU and international legal framework governing online violations of privacy and data protection through a criminal law lens. In this context, it examines closely the crimes of illegal access, illegal interception, data interference, system interference and misuse of devices.

Finally, the liability of digital platforms will also be addressed, in order to examine whether the legal framework that applies to intermediary service providers of information society services is adequate, when it comes to cybercrime.

Resumo

Num contexto em que a pegada digital se torna progressivamente "maior" do que a física, todos acedem facilmente aos bens e serviços oferecidos em linha. Contudo, ao mesmo tempo, novas ferramentas tecnológicas, tais como os *smartphones*, tornam os utilizadores da *World Wide Web* mais vulneráveis a intrusões na sua esfera de privacidade.

As violações à privacidade, tais como a interceção ilegal, podem comprometer a segurança do utilizador tanto *online* como *offline*, expondo-o a um dano considerável, muitas vezes causado por um agente cujo rastreio não é possível. Além disso, a falta de conhecimento tanto dos riscos que os utilizadores da Internet enfrentam como das medidas de proteção que podem tomar para enfrentar esses riscos aumenta significativamente a sua vulnerabilidade.

Neste contexto, esta tese examinará o *status quo* do cibercrime - com foco nos elementos que o distinguem do crime offline: o anonimato do agente, o seu alcance global e a possibilidade de redimensionamento, a transnacionalidade do cibercrime, bem como as dificuldades de o abordar através de uma regulamentação robusta e imutável.

Além disso, esta tese aprofunda o quadro jurídico da UE e internacional que rege as violações da privacidade e da proteção de dados em linha através da lente do direito penal. Neste contexto, examina de perto os crimes de acesso ilegal, interceção ilegal, interferência de dados, interferência de sistemas e utilização indevida de dispositivos.

Finalmente, a responsabilidade das plataformas digitais será também abordada, a fim de examinar se o quadro jurídico aplicável aos prestadores de serviços intermediários da sociedade da informação é adequado, quando se trata de cibercriminalidade.

TABLE OF CONTENTS

I. INTRODUCTION

The rights to privacy and protection of personal data are fundamental rights enshrined in the Charter of Fundamental Rights of the European Union (CFREU)[1]. Nowadays, given the specific features of cyberspace, such as the possibility for the perpetrator to stay anonymous and to impact a large number of people easily, and the lack of space and time barriers (among other risk factors), the protection of these rights is one of the biggest challenges legislators, law enforcement and judicial authorities face.

Additionally, one shall take into consideration that the dependency of individuals on technology evolves at an extraordinarily quick pace[2]. If the existing (inter-)connected infrastructures ever fail, many vital tasks may not be performed; for instance, online banking services and cell phone communications would be interrupted. The same applies to social media – irrespective of the importance one ascribes to them.

If the Internet were indeed the "*no-man's land*"[3] advertised in the 1996 "*Declaration of the Independence of Cyberspace*"[4], a great portion of businesses and fundamental rights of internet users would be left unattended.

Considering the amount of IP addresses connected through the web as well as the vital role of the internet in the everyday life of the average citizen, it would be imprudent to leave the World Wide Web unregulated, especially as regards cases that amount to a considerable violation of legal interests, and particularly those protected by means of criminal law.

Online crimes correspond, to some extent, to offline ones, in terms of the conduct they aim to prevent. This is, for instance, the case with data breach and theft,

---

[1] European Union, "Charter of Fundamental Rights (2012/C 326/02)", Articles 7 and 8.
[2] Mike Keyser, "The Council of Europe Convention on Cybercrime", 12 J. Transnat'l L. & Pol'y 287 (2002-2003), available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jtrnlwp12&div=14&id=&page= (last access on 29.10.2021), 2003, p. 290.
[3] Jeff Kosseff, "8. A Lawless No-Man's Land?" In The Twenty-Six Words That Created the Internet, 167-189. Ithaca, NY: Cornell University Press, available at: https://doi.org/10.7591/9781501735783-010 (last access on 29.10.2021), 2019, p. 167.
[4] John Perry Barlow, "A Declaration of the Independence of Cyberspace", John Perry Barlow Library, available at: https://www.eff.org/cyberspace-independence (last access on 29.10.2021), 1996.

which were both conceived to prevent intrusions into property. However, despite the similarities, the specific characteristics of the online context add a layer of complexity to cybercrimes, increasing the level of risk the victims face and providing new opportunities and a new structure for the perpetrator to explore. These special elements which are responsible for the additional layer of complexity that characterizes cybercrime are to be analysed in turn.

One of the existing criminological theories which can be used to elaborate on how these special elements interact with the main motives which lead perpetrators to incur in criminal activity, is the Routine Activity Theory (RAT). Even though that theory was designed to apply to offline criminal activity, the author is of the opinion it can be deployed to explain the commission of crimes in the cyberspace. That theory is chosen, as, first, it has been used for a long period of time to analyse several kinds of criminal behaviour and second, it is flexible enough to cover a rather wide set of criminal scenarios, such as the online one[5].

New technologies have reshaped routine activities massively[6]. For instance, the vast majority of desk jobs, which would require using books and a great number of dossiers, now depend on information available online and computer storage capacity. Digitalisation has also impacted on leisure (e.g., watching movies online) and economic activities (e.g., shopping online). Hence, RAT (if applied) may be used to explain the impact of those new routine activities on criminality.

Cohen and Felson developed their theory around 1979, in a post Second World War scenario, where criminal rates in the US were trending upwards[7]. In their words, there are three minimal elements necessary in each direct-contact predatory violation: "*(1) motivated offenders, (2) suitable targets, and (3) the*

[5] Eric Rutger Leukfeldt & Majid Yar: "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis", available at: http://dx.doi.org/10.1080/01639625.2015.1012409 (last access on 29.10.2021), 2016, p. 263, 264.
[6] Bradford W. Reyns, "Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses", Journal of Research in Crime and Delinquency 50, no. 2 216–38, available at: https://doi.org/10.1177/0022427811425539(last access on 29.10.2021), 2013, p. 220.
[7] *Ibidem*, p. 220.

absence of capable guardians against a violation" [8]. The absence of any of these elements is sufficient to prevent the successful completion of the crime.

As for the first element, the *motivated offenders*, it is important to note that the perpetrators are particularly motivated by the specific conditions provided by the cyberspace. First, cybercriminals may work from the comfort of their homes and do not have to necessarily reveal themselves to the world, suffering from the condemnation of others, as there are many anonymizing tools available online (which will be presented in Section II). Second, cybercrime is not attached to a specific space and the traditional perception of time. The same perpetrator can commit millions of crimes at the same time, in various locations, through the same connected device, having the said "*Global Reach"*[9]. This omnipresence factor facilitates the scalability of cybercrime, as it enables the perpetrator to access a wide number of people around the globe. Through a single click, the perpetrator is capable of committing a large number of crimes against a proportionally large number of victims[10]. In other words, the cyberspace provides cybercriminals with the opportunity to reach millions of individuals from all around the globe, breaking the barriers of time and distance.

Besides this, the cybercriminal may be motivated by the lack of cybercrime reporting, as it is estimated that 80% of the victims do not report to the competent authorities[11]. This trend is associated with various factors, among which it is important to highlight that more often than not, cybercrimes, when individually considered, do not have the necessary impact for the victims to take action, or to even notice the commission of the crime.

---

[8] Lawrence E. Cohen & Marcus Felsen, "Social Change and Crime Rate Trends: a Routine Activity Approach", American Sociological Review 1979, Vol. 44 (August), available at: http://www.personal.psu.edu/users/e/x/exs44/597b-Comm%26Crime/Cohen_FelsonRoutine-Activities.pdf(last access on 29.10.2021), 1979, p. 589.

[9] Bert-Jaap Koops, "The Internet and its Opportunities for Cybercrime", TRANSNATIONAL CRIMINOLOGY MANUAL, M. Herzog-Evans, ed., Vol. 1, pp. 735-754, Nijmegen: WLP, 2010; Tilburg Law School Research Paper No. 09/2011, available at https://ssrn.com/abstract=1738223 (last access on 29.10.2021), 2011, p. 740.

[10] Majid Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory", European Journal of Criminology 2, no. 4 (October 2005): 407–27, available at: https://doi.org/10.1177/147737080556056 (last access on 29.10.2021), 2005, p. 421.

[11] UNODC United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime", available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (last access on 29.10.2021), 2013, p.13.

Additionally, considering the evolution of technologies (whether incorporated in everyday gadgets or intangible, such as digital platforms capable of providing the most varied services), their accessibility all around the world and the proportional increase of the number of people interested in studying or exploring opportunities to monetize reprovable behaviours, assuming the role of a hacker or a cracker is possible for more and more people, as new generations adapt to this new reality.

In this context, even though no mathematical study capable of supporting this argument has been conducted by the author, through a syllogistic line of argumentation it shall be concluded that cyberspace provides the offender with an extra level of motivation to commit crimes against the privacy of citizens.

If the motivation of the offender with criminal inclinations and the ability to follow such inclinations are indispensable elements for illicit activities to occur; and if cyberspace has a whole set of enticing features for the offender that are not present in the offline world; Then cyberspace provides the perpetrator with an additional layer of motivation, which contributes to an increase in his *willingness* to commit crimes.

In sum, the author is of the opinion that cybercriminals will be able, based on the routine activities established in our society, to foresee that he will be less likely to be judged and prosecuted, both by society and by the competent authority, if he commits a cybercrime, than if he had committed a crime without the involvement of the technological medium.

As for the second element, i.e., that of *suitable targets*, it is worth beginning by noting that not only the average citizen, but also powerful economic operators, such as big corporations, may become the victim of cybercriminals. In accordance with RATs, there are four elements capable of making a target more suitable: value, inertia, visibility, and accessibility (VIVA) - with Cohen and Felsen concluding back at that time that "*expensive movable durables, such as vehicles and electronic appliances have the highest risk of illegal removal*"[12].

[12] Lawrence E. Cohen & Marcus Felsen, "Social Change and Crime Rate Trends: a Routine Activity Approach", American Sociological Review 1979, Vol. 44 (August), available at: http://www.personal.psu.edu/users/e/x/exs44/597b-Comm%26Crime/Cohen_FelsonRoutine-Activities.pdf (last access on 29.10.2021), 1979, p. 595.

The meaning of VIVA is considerably different in the online environment. The 'value' stands for the commercial value of a given piece of data or confidential information[13]. In the offline world, the term 'inertia' refers to the properties of objects or persons incapable of offering resistance to an attack[14]. When transposed to cyberspace, it may represent the *volume* of the stolen data (e.g., just like an heavy car is more difficult to steal than a golden plate, a file with multiple terabytes will be more challenging to transfer than a 100kb one) as well as the characteristics of the utensils or means used by the perpetrator, such as the storage capacity and computational power of the computer used to misappropriate data or confidential information[15]. 'Visibility', when examined in the online context, stands for the extent to which a given person exposes him/herself online[16]. Finally, in the offline context, the term 'accessibility' refers to those circumstances that make it easier for the offender to contact the target, such as the placement of goods in reachable locations. In cyberspace, it would mean the level of weakness of the software or operating system of a given connected device – with systems presenting a low level of protection and security barriers becoming more accessible to perpetrators[17].

Still on the subject of the target suitability of data subjects, it should be noted that one of the main problems is that data subjects are not really aware of the dangers associate with a low-level protection of their personal data. According to the latest Eurobarometer statistics on Europeans' attitudes towards cybersecurity, 76% of the EU inquired citizens believe there is an increasing risk of being a victim of cybercrime[18]. However, even though data subjects are aware of the existence of cybercrimes, it is possible to affirm they are more concerned with the possibility of being robbed than having all their devices hacked at once. It is common sense that one is not supposed to carry around an open purse in a crowded place, and,

[13] Eric Rutger Leukfeldt & Majid Yar: "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis", available at: http://dx.doi.org/10.1080/01639625.2015.1012409 (last access on 29.10.2021), 2016, p. 269.
[14] Majid Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory", European Journal of Criminology 2, no. 4 (October 2005): 407–27, available at: https://doi.org/10.1177/147737080556056 (last access on 29.10.2021), 2005, p. 420.
[15] *Ibidem*, p.420.
[16] *Ibidem*, p.270.
[17] *Ibidem*, p.270.
[18] Special Eurobarometer 499, Europeans' attitudes towards cyber security, available at: https://op.europa.eu/pt/publication-detail/-/publication/468848fa-49bb-11ea-8aa5-01aa75ed71a1 (last access on 29.10.2021), 2020, p. 6.

therefore, (s)he takes preventative measures to avoid getting robbed. On the contrary, setting a different password for each account or setting up a two-factor authentication system looks like a time-consuming preventive measure for those who are in fact aware about the dangers they face in cyberspace and that such preventive measures are at their disposal. Due to lack of information, most data subjects usually do not take the necessary precautions to prevent data related cybercrimes and, thus, become suitable targets.

The third element, namely the *absence of "capable guardianship",* refers to "*the capability of persons and objects to prevent crime from occurring*"[19]. In cyberspace, prevention can assume different forms, both formal or informal, physical or abstract. Those include, for instance, the supervision of children navigating on the web by an adult, the tasks taken one by law enforcement agencies aiming to prevent and to prosecute criminal activities, and even the inhouse network administrators and security staff who supervise the software and the hardware of a given entity[20]. Guardianship in cyberspace might also take the form of physical technological security measures, namely automated technology programmed to execute a continuous supervision, such as an anti-virus software, email filters and even two-factor authentication systems for passwords[21]. These technological security measures may mitigate the risks of navigating on the web. On other hand, the lack of vigilance on behalf of users, provides the perfect conditions for being targeted, *inter alia*, for some sort of intrusion into their personal data.

Some of the riskiest behaviours frequently adopted by web users is the use of public networks (e.g., in coffee shops or libraries)[22], especially when typing sensitive information, since this provides a window of opportunity to all motivated

[19] Tseloni Andromachi, Karin Wittebrood, Graham Farrell, & Ken Pease, "Burglary Victimization in England and Wales, the United States and the Netherlands: A Cross-National Comparative Test of Routine Activities and Lifestyle Theories." The British Journal of Criminology 44, no. 1 (2004): 66-91, available at: http://www.jstor.org/stable/23639022 (last access on 29.10.2021), p. 74.
[20] Majid Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory", European Journal of Criminology 2, no. 4 (October 2005): 407–27, available at: https://doi.org/10.1177/147737080556056 (last access on 29.10.2021), 2005, p 423.
[21] Ming-Li Hsieh & Shun-Yung Kevin Wang, "Routine Activities in a Virtual Space: A Taiwanese Case of an ATM Hacking Spree". International Journal of Cyber Criminology, 12(1), 333–352, available at: https://doi.org/10.5281/zenodo.1467935Hsieh (last access on 29.10.2021), 2018, p. 338.
[22] *Ibidem*.

offenders, who are in the same network, to access the victim's computer, and all personal data stored there. Setting the same password for all social media accounts and not changing passwords regularly also involve a great risk. This implies that individuals often put themselves at a great risk of being hacked without realizing it.

In parallel, similar to what happens in the offline world, the maintenance of a formal social guardian, such as the police, on a twenty-four-seven basis, is highly impossible from a scaling perspective. Additionally, cyberspace makes such a measure rather ineffective, given the lack of spatial barriers and the ease the perpetrators have in virtually relocating the place where the crime was committed[23].

Against this backdrop, RAT appears as a flexible tool capable of fitting the unique shape of cybercrime and explaining cyber-criminality. We are indeed experiencing a different time and space perception, but the basic elements which sustain the problem remain the same. With that in mind, one might ask: Should this new approach to the same ancient elements differ so much? Or should we just try to fit "*old wine*"[24] in these very innovative bottles?

Turning the spotlight to online violations of privacy and data protection, which are the focal point of this thesis, as shown by surveys[25], they represent a subject matter that clearly needs new solutions and approaches.

Ever since data has intrinsic value, online data protection violations have increased[26]. According to empirical studies, personal data is the most commonly

[23] *Ibidem*, p.344.
[24] Susan W. Brenner, "Cybercrime Metrics: Old Wine, New Bottles?", Virginia Journal Of Law & Technology Fall 2004 University Of Virginia Vol. 9, No. 13, available at: https://www.researchgate.net/publication/265032559_Cybercrime_Metrics_Old_Wine_New_Bottles/stats (last access on 29.10.2021), 2004, p. 8
[25] Namely, the public consultation organized by the European Commission in 2016, in the context of the drafting of the proposal for the ePrivacy Regulation, which illustrated that 83.4% of the responding citizens, consumer and civil society organisations and 88.9% of public authorities agreed on the need for special rules for the electronic communications sector on confidentiality of electronic communications (*in* European Parliament & Council, "Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN (last access on 29.10.2021), 2017, p. 6.)
[26] Rob Sobers, "98 Must-Know Data Breach Statistics for 2021", Varonis, 4. 16, 2021, available at https://www.varonis.com/blog/data-breach-statistics/ (last accessed on 29.10.2021), 2021.

compromised type of data, followed by payment data and medical data[27]. The main reason for this is the huge amount of personal data collected, retained and processed, all over the Internet. Now more than ever, people feel the need to share personal matters with others through social media, making it easier for criminals to access, collect and misuse their data[28].

Big Data[29], Data Mining[30] and Data Analytics[31] are transforming crime, both for better and for worse. On the bright side, law enforcement agents are using such innovative tools to create behaviour patterns with the aim of preventing and controlling crime more efficiently[32]. On the flip side, criminals also exploit these tools for their own purposes, allowing them to process and categorize huge amounts of data through less time-consuming processes[33].

As a response to the increase in data breaches, many international (e.g., the Budapest Convention on Cybercrime, EU (e.g., the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014) and national laws have been adopted to criminalize behaviours threatening privacy online. Besides this,

---

[27] Europol, "Internet Organised Crime Threat Assessment" (Iocta), available at: https://perma.cc/N8HQ-CZT9 (last access on 29.10.2021), 2018, p.22.

[28] Ralph Gross & Alessandro Acquisti, "Information Revelation and Privacy in Online Social Networks (The Facebook case)." Paper presented at the meeting of the ACM Workshop on Privacy in the Electronic Society (WPES), Alexandria, available at: https://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf (last access on 29.10.2021), 2005, p. 1.

[29] In accordance with Investopedia, the concept of Big Data "*refers to the large, diverse sets of information that grow at ever-increasing rates. It encompasses the volume of information, the velocity or speed at which it is created and collected, and the variety or scope of the data points being covered (…). Big data often comes from data mining and arrives in multiple formats*.", further notes on the definition are available at: https://www.investopedia.com/terms/b/big-data.asp (last access on 29.10.2021).

[30] In accordance with Investopedia, the concept of Data Mining refers to "*a process used by companies to turn raw data into useful information. By using software to look for patterns in large batches of data, businesses can learn more about their customers to develop more effective marketing strategies, increase sales and decrease costs.",* further notes on the definition are available at: https://www.investopedia.com/terms/d/datamining.asp (last access on 29.10.2021).

[31] In accordance with Investopedia, the concept of Data Analytics "*is the science of analyzing raw data to make conclusions about that information. Many of the techniques and processes of data analytics have been automated into mechanical processes and algorithms that work over raw data for human consumption*.", further notes on the definition are available at: https://www.investopedia.com/terms/d/data-analytics.asp (last access on 29.10.2021).

[32] Andrii Shalaginov, Jan William Johnsen & Katrin Franke, Cyber crime investigations in the era of big data", 2017 IEEE International Conference on Big Data, available at: https://www.researchgate.net/publication/322511369_Cyber_crime_investigations_in_the_era_of_big_data 2017 (last access on 29.10.2021), p. 2.

[33] Sofia Agostinho, "Online Violations of Data Protection – The Criminal Law Perspective", Essay submitted at Nova School of Law in the context of the Course "Cybersecurity", Spring Semester 2020, p. 2.

many of these reprehensible behaviours are subject to administrative and civil sanctions [as provided, for instance, in the General Data Protection Regulation (hereinafter "*GDPR*")][34].

In this context, when seeking to address such an innovative problem by employing one the most traditional means of legal regulation, namely *criminal law*, several obstacles arise. For instance, concepts like "*possession*" or "*theft*", which are commonly used in substantive criminal law, were conceived to be applied to the physical world, and not the virtual one[35]. Additionally, the anonymity of the offender, the transnationality of cybercrime, the possibility to have a global reach with a click, the different perception of time and space and the option to forum shopping, makes the legislator's role really complicated[3637].

Some decades ago, organizing the online bubble and the physical world in two separate boxes might have been feasible. However, to increase the struggle of regulating cyberspace even further, in the digital era, the Internet has control not only over tablets, cell phones and computers, but also over most of the objects one uses in daily life (e.g., smart tv and even smart houses). Most Internet-of-Things (IoT) traffic is unencrypted, which ends up exposing personal data on the network and data subjects to cyber-attacks[38]. The IoT bridged the gap between

[34] European Parliament & Council, "Regulation (EU) 2016/679 of the 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)", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN(last access on 29.10.2021), 2016.

[35] Aleš Završnik, "Towards an overregulated cyberspace: criminal law perspective", Masaryk University journal of law and technology, available at: https://journals.muni.cz/mujlt/article/viewFile/2566/2130(last access on 29.10.2021), 2010, p. 183.

[36] Bert-Jaap Koops, "The Internet and its Opportunities for Cybercrime", TRANSNATIONAL CRIMINOLOGY MANUAL, M. Herzog-Evans, ed., Vol. 1, pp. 735-754, Nijmegen: WLP, 2010; Tilburg Law School Research Paper No. 09/2011. Available at https://ssrn.com/abstract=1738223(last access on 29.10.2021), 2011, p. 740, 741.

[37] Sofia Agostinho, "Online Violations of Data Protection – The Criminal Law Perspective", Essay submitted at Nova School of Law in the context of the Course "Cybersecurity", Spring Semester 2020, p. 2.

[38] Mohan Krishna Kagita, Navod Thilakarathne, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, & Saurabh Singh, "A Review on Cyber Crimes on the Internet of Things", in: ResearchGate, available at: https://www.researchgate.net/publication/344244881_A_Review_on_Cyber_Crimes_on_the_Internet_of_Things (last access on 29.10.2021), 2020, p. 3, 4.

cyberspace and the real world, making the latter susceptible to all kinds of cyber-attacks[39].

"*Cybercrime is real crime, and increasingly, real crime has a cyber-element to it*"[40]- making data related cybercrimes worthy of analysis. While the current, new-technologies-driven reality has proven to be extremely beneficial in fostering people's proximity, all these developments also carry the same weight in terms of negativity and risk for the privacy and security of citizens and economic operators. Against this backdrop, this thesis will explore the legal response to online violations of privacy and data protection – mostly from a substantive-criminal-law point of view.

In *Section II*, the characteristics of cyberspace that make it adverse to a purely theoretical or conceptual approach by criminal law will be studied in depth. In this context, transnationality, scalability, anonymity, the lack of information and awareness of Internet users, the possibility to resort to organised crime without even having to rely on a physical gathering of criminals will be further examined. *Section III* will introduce the main types of crimes regulated in several international and EU laws that protect privacy and personal data, namely, the crimes typified in the Budapest Convention[41] and in the EU Directive on attacks against information systems[42] as well as the provisions of the GDPR, which provide for the possibility to criminalize data protection violations. In this regard, the potential legal framework for personal data will be also analysed. More specifically, this thesis will address the question of whether such data should be perceived and regulated as property of the data subject, an autonomously protected legal good, a fundamental right or a *tertium genus* worthy of a hybrid

[39]Deloitte, "Cyber risk in an Internet of Things world Flashpoint edition 4: More data, more opportunity, more risk", available at: https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html (last access on 29.10.2021), p. 1.

[40] Bert-Jaap Koops, "Criminal law and cyberspace as a challenge for legal research", In: SCRIPTed, Vol. 9, No. 3, 2012, available at: http://script-ed.org/wp-content/uploads/2012/12/koops.pdf (last access on 29.10.2021), 2012, p. 355

[41] Council of Europe "Convention on Cybercrime" hereinafter referred to as "CoE Convention", available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008156l (last access on 29.10.2021), 2001.

[42] European Parliament and Council, "Directive 2013/40/ on attacks against information systems and replacing Council Framework Decision 2005/222/JHA", available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040 (last access on 29.10.2021), 2013.

regime. In the same section, it will also be examined which is the best system to penalise cybercrimes, i.e., whether the legislator should try to fit cybercrimes in already existing types of crime or rather create new types of crime. Besides this, it will be examined whether the impact of the already typified cybercrimes is significant enough to justify the intervention of criminal law. The criminal liability of electronic communication service providers and digital platforms for online violations of privacy and data protection will be addressed in *Section IV*. There, it will also be examined which are their obligations, in the light of the legislation, whether currently in force or to be transposed in the near future (e.g., Digital Services Act)[43].

With that in mind, the main goal of this thesis is to examine the key characteristics of cyberspace, the current approach to data related cybercrimes adopted in international and EU law and to propose some alternative solutions to the problems associated with the fight against cybercrime and online privacy and data protection violations in particular.

[43] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 2020", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en(last access on 29.10.2021), 2020.

II. THE CHALLENGES OF CYBERCRIME

a. Risk Factors

Cyberspace is "*a global network, [which] provides for instantaneous connections, in a networked structure that is decentralized, and it is based on digital representation of information*"[44]. According to Koops, there is a set of risk factors inherent to cyberspace[45], which will be the main subject of the following analysis.

Such risk factors include the internet's "*global reach";* its *"deterritorialization"*; the scalability of cybercrime; the flexibility of its *decentralized networks* which facilitate the commission of organized crime; the notorious "*absence of capable guardians";* the possibility for the perpetrator to remain anonymous for the entire process of the crime commission; the possibility to enable "*distant interaction with victims"*; *the "manipulability of data and software with minimal cost";* the fact that it allows for "*automation of criminal processes where one piece of software can replicate and attack millions of computers at the same time";* the evolutionary capacity of technologies, which make it difficult to keep up with legislative and bureaucratic procedures and diplomas – the "*pacing problem*"[46]; and the fact that the structure of the Word Wide Web allows the perpetrator to commit billions of minor and nearly irrelevant crimes towards billions of internet users, from which the criminal may retrieve a substantial economic gain, without the typical proportional loss of the counterparty[47].

Some of these elements have already been analysed above, on the subject of the Routine Activity Theories. With that in mind, this chapter will merely focus on

[44] Bert-Jaap Koops, "The Internet and its Opportunities for Cybercrime", TRANSNATIONAL CRIMINOLOGY MANUAL, M. Herzog-Evans, ed., Vol. 1, pp. 735-754, Nijmegen: WLP, 2010; Tilburg Law School Research Paper No. 09/2011. Available at: https://ssrn.com/abstract=1738223 (last access on 29.10.2021), 2011, p.738.
[45] *Ibidem*, p. 740, 741.
[46] Gary Elvin Marchant, Braden R Allenby & Joseph R Herkert, "The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem", Springer Netherlands Available at: https://www.springer.com/gp/book/9789400713550 (last access on 29.10.2021), 2011.
[47] Bert-Jaap Koops, "The Internet and its Opportunities for Cybercrime", TRANSNATIONAL CRIMINOLOGY MANUAL, M. Herzog-Evans, ed., Vol. 1, pp. 735-754, Nijmegen: WLP, 2010; Tilburg Law School Research Paper No. 09/2011. Available at: https://ssrn.com/abstract=1738223 (last access on), 2011, p. 740, 741.

some of the remaining elements, which the author considers the most impactful in this context.

i. Anonymity

The anonymity is one of the most attractive characteristics of cyberspace for the perpetrator, who may conceal the criminal act from those who are closer to him, avoiding the burdens of public scrutiny.

On the internet, not only anonymity is easily achievable, but also pseudoanonymity. The concept of online anonymity refers to situations where the identity of a person acting on the internet is not possible to uncover through any method. Pseudoanonymity, on the other hand, refers to the cases where it is possible to unveil the identity of a person[48].

In this context, some of the tools frequently used by offenders to veil someone's identity are proxy servers. These virtual instruments are capable of hiding the IP's identity using techniques which make it quite difficult and definitely time-consuming for law enforcement agencies to trace and unveil the offender's identity. This goes as follows: the perpetrator uses the proxy to establish a connection between his computer and some other IP address, which belongs to the last person who visited a given website. During this technology driven process, both the identification of the perpetrator and the command sent from his computer to the proxy server are hidden. For this reason, all his actions on the web henceforth, will be mostly anonymized and untraceable[49].

Some other means perpetrators may use to conceal their identity are remailers, spoofed email and torrent[50]. An anonymous remailer is a server that, upon receiving an email, removes the identification of the sender and directs the intended message to the addressee specified by the sender. Depending on the skills of the internet user, remailers can achieve 100% anonymity, making it an

[48] Kamal Ahmad & UNITAR, "The law of cyber-space : an invitation to the table of negotiations", United Nations Digital Library, available at: https://digitallibrary.un.org/record/566838 (last access on 29.10.2021), 2005, p. 23,24.
[49] Jeff Petters, "What is a Proxy Server and How Does it Work?", available at: https://www.varonis.com/blog/what-is-a-proxy-server/ (last access on 29.10.2021), 2021.
[50] *Ibidem*, p. 26.

untraceable means of communication, providing suitable channels for perpetrators to communicate with each other and to orchestrate organised criminal acts[51].

Additionally, some examples of anonymity networks are Freenet, and the Invisible Internet Project[52] (known as I2P)[53].

On this topic, the Council of Europe (hereinafter "*CoE*") has established broad recommendations for both Users and Internet Service Providers (hereinafter "*ISP*"), in its Recommendation N (99) R 5[54].

As for Users, the CoE stated that all transactions made by users, as well as all the visited sites leave traces or "*electronic tracks*", which can be used, regardless of the user's awareness or knowledge, to build profiles which categorize the user and its interests, so that personalized adds and services can be provided accordingly.

If users do not wish to be profiled, they must use appropriate technical means, including being informed by each ISP of the fact their visit to a given site is leaving traces and that they may reject such traces if they prefer. The Recommendation under analysis also recommends users to search and ask for the privacy policy of the browsed sites and programmes and to prefer those who record and process few data. Another possibility foreseen in the Recommendation is to access websites and use services anonymously[55].

One of the already available tools for this purpose is the Tor Browser, which consists of a downloadable software, capable of isolating each accessed website

---

[51] *Ibidem*, p. 22.

[52] Freenet is a "*peer-to-peer platform for censorship-resistant communication and publishing",* where "*Browse websites, post on forums, and publish files within Freenet with strong privacy protections*" – Freenet Project, available at: https://freenetproject.org/ (last access on 29.10.2021). On the other hand, the Invisible Internet Project is an "*encrypted private network layer*" - The Invisible Internet Project, available at: https://geti2p.net/en/ (last access on 29.10.2021).

[53] UNDOC, "Obstacles to cybercrime investigations", available at: https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html (last access on 29.10.2021), 2019.

[54] Council of Europe, "Recommendation N (99R) 5 of Council of Europe Committee of Ministers of the Committee of Ministers to Member States for the Protection of Privacy on the Internet", available at: https://www.fd.unl.pt/docentes_docs/ma/MEG_MA_4009.pdf (last access on 29.10.2021), 1999.

[55] *Ibidem*, p. 3.

so trackers and targeted advertisement cannot follow a given user's IP address. It is basically a free network designed to anonymise the user's real IP address by routing the user's traffic through many servers of the Tor network. Tor is used by a variety of people for both illicit and licit purposes. Additionally, this tool provides the opportunity for users to appear alike, making it difficult for them resistible to fingerprinting[56].

However, the CoE also refers that complete anonymity may not always be the most suitable option – for instance, for tax purposes, it is important that users identify themselves when making a transaction. Additionally, incentivising total anonymity would encourage cybercriminals to hide their identity when committing crimes, as they would be led to believe they were merely following the Council of Europe's Recommendations. For the cases where anonymity may not be the most suitable option, the CoE recommends the use of pseudonyms when permitted by law. Despite the efforts of the Council of Europe, no further guidance is provided to help users define the situations where anonymity may not be the most suitable option[57].

As for ISP, the CoE refers that they must inform their users about the possibility to access the Internet, use and pay for its services anonymously (for example through the use of pre-paid access cards), before accepting such user's subscription and connection to the Internet[58].

However, the CoE, once again, mentions that complete anonymity may not be the most suitable option because of legal constraints. In that case, it suggests the use of pseudonyms when permitted by law. Finally, the CoE recommends these economic operators to design their system is a way which is capable of avoiding or minimizing the use of personal data[59].

[56] Tor Project, "Browse Privately. Explore Freely.", https://www.torproject.org/ (last access on 29.10.2021).
[57] Council of Europe, "Recommendation N (99R) 5 of Council of Europe Committee of Ministers of the Committee of Ministers to Member States for the Protection of Privacy on the Internet", available at: https://www.fd.unl.pt/docentes_docs/ma/MEG_MA_4009.pdf (last access on 29.10.2021), 1999, p.3.
[58] *Ibidem*, p. 4.
[59] *Ibidem,* p.4.

In this context it is possible to affirm that, even though, in practical terms, these postulates have little or no applicability, the first steps towards a safe and informed browsing on the World Wide Web have already been taken.

Without prejudice, as this postulate is nothing more than a recommendation, it remains to be seen whether the next laws that regulate the realm of information technologies and the imperious need of privacy on the part of their users, will adopt or incorporate such recommendations in a more imperative way.

In the author's opinion, the desirable outcome would be to impose on economic operators, an effective obligation to enable tools which allow the pseudonymisation or anonymization of each data subject browsing on their websites or programmes, when legally allowed. Only then would ISP truly be incentivized to provide the tools which allow internet users to use the services in a way that their right to privacy is not completely disregarded.

The next opportunity for the EU regulator to properly approach this theme will be the ePrivacy regulation.

Within the scope of the proposal for this Regulation, which has already been published by the European Commission[60], Chapter III deserves special mention, since it concerns "*the rights of end-users to control the sending and reception of electronic communications to protect their privacy*"[61].

That said, even though anonymity may be a desirable goal to ensure users' privacy, it may as well be used to conceal the identity of perpetrators, making it more difficult to prosecute them. The time-consuming back-tracing process through which public authorities unveil the perpetrator's identity, provides the perpetrator with precious time to commit several other intrusions, making it hard for such authorities to gather the relevant proof and prosecute him for all of them[62].

---

[60] European Parliament & Council, "Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN (last access on 29.10.2021), 2017, p. 9, 28, 29.

[61] *Ibidem*, p. 9.

[62] Howard F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues", Software Engineering Institute, available at:

This results in a huge cybercrime enforcement gap[63]- the percentage of incidents that occur annually is way bigger than those that result in an arrest.

One of the already proposed solutions would be the implementation of an Internet Protocol which conceded one unique identifier attached to every computer's or connected device IP address, which could not be reaped apart from the communications and transactions conducted online[64].

Additionally, it would be useful to legally impose on service providers, the duty to keep an encrypted record of all communications sent by all these permanently attached IP addresses, as a kind of black box, available only to enforcement authorities and merely upon sustained request, forwarded to the economic operator's Data Protection Officer.

It is undeniable that such a solution would often be perceived as an unjustified intrusion into people's privacy and freedom of speech. However, one must not forget that Data Protection Officers are bounded by special duties of confidentiality and must not be treated as subordinated workers, namely they must not receive any instructions from a superior of any kind regarding the development of their tasks[65].

With that in mind, the intrusion on people's privacy would necessarily have to be kept to the minimum indispensable and it would actually be justified by the need to keep the data subjects safe while browsing the web.

In order to keep such intrusion to a minimum, objective standards would have to be defined, determining which cases are relevant enough to open the said "b*lack box*". Some guiding principles could be the scale and impact of a said cybercrime.

https://resources.sei.cmu.edu/asset_files/SpecialReport/2002_003_001_13928.pdf (last access on 29.10.2021), 2002, p. 4.

[63] Allison Peters & Amy Jordan, "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime", available at: https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime (last access on 29.10.2021), 2019, p.490.

[64] Kamal Ahmad & UNITAR, "The law of cyber-space: an invitation to the table of negotiations", United Nations Digital Library, available at: https://digitallibrary.un.org/record/566838 (last access on 29.10.2021), 2005, p. 25, 26.

[65] As provided for in Article 38 of the GDPR.

ii. Transnationality

An extra layer of complexity is added to the process of prosecuting the perpetrator, when the cybercriminal decides to store data in numerous jurisdictions, some of which are safe-havens[66], where certain technology driven crimes are not typified. A representative example of a so-called "*safe-haven*", is the Central African Republic, where, according to the UN records, no cybercrime or data protection laws are in place[67].

As technological developments make it possible to change the location, where one acts, the window of opportunity for cybercriminals becomes evident.

If the territoriality principle (which will be further developed below) is applied to cybercrime, this creates the possibility for someone to change their IP's location through a VPN, thus making it seem that they are operating on a country where a certain conduct is not criminalized. This means that, for example, a German hacker can work from the comfort of his home and make it seem that he is in Central African Republic so that he cannot be prosecuted for his actions.

A case which perfectly illustrates the idea of safe-havens is the one of the "*I Love You*" virus[68], which affected fifty million devices, but did not lead to an enforcement decision, despite the identification of the offender. The latter was tracked in Philippines, where his conduct was not punished as a crime back at that time[69].

[66] UNODC United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime", available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (last access on 29.10.2021), 2013, p. 93.

[67] UNCTAD, "Cybercrime Legislation Worldwide", available at: https://unctad.org/page/cybercrime-legislation-worldwide (last access on 29.10.2021), 2020.

[68] Davey Winder, "This 20-Year-Old Virus Infected 50 Million Windows Computers In 10 Days: Why The ILOVEYOU Pandemic Matters In 2020", Forbes Magazine, available at: https://www.forbes.com/sites/daveywinder/2020/05/04/this-20-year-old-virus-infected-50-million-windows-computers-in-10-days-why-the-iloveyou-pandemic-matters-in-2020/ (last access on 29.10.2021), 2019, paragraph 1.

[69] Amalie W. Weber, "The Council of Europe's Convention on Cybercrime", Berkeley Technology Law Journal Vol. 18, No. 1, Annual Review of Law and Technology (2003), pp. 425-446 (22 pages) Published By: University of California, Berkeley, School of Law, available at: https://www.jstor.org/stable/24120528 (last access on 29.10.2021), 2003, p.426.

In such context, the harmonization of cybercrime appears to be of key importance. International Conventions play an important role inasmuch as they define the minimum limits of what must be punished in all signatory countries.

Given the transnationality of cyberspace, it is absolutely necessary to establish a connection principle capable of linking a crime to a certain jurisdiction. The principle commonly used to connect a crime to a certain jurisdiction is the one of *territoriality*, according to which a given conduct will be prosecuted by a certain state if the act is committed within that state's territorial borders[70].

The link between a crime and a certain jurisdiction may be also established on the basis of the *flag* principle, the principle of *objective territoriality* and the so-called *active nationality* principle.

The flag principle acts as an extension to the territoriality principle and refers to the cases where the offence is committed on board of a ship or aircraft situated outside the terrestrial jurisdiction of a given country, as such ships and aircrafts are, more often than not, deemed as an extension of the territory of the nation[71]. The principle of objective territoriality further extends the concept of territoriality to those situations where criminal conduct actually has a substantial effect in a given jurisdiction[72].

The active nationality principle, stipulates that a given nation has jurisdiction over a certain crime, in case that the crime is committed by one of its nationals. In accordance with the Convention on Cybercrime, this last principle requires a double condition, since for it to apply, the conduct must not only be criminalized under the laws of the country of nationality of the perpetrator, but also those where he/she effectively practiced the act at stake. The assumption here is that every citizen should be obliged to comply with the laws of his country of nationality, even when they are outside their territory[73]. The purpose of this

[70] Uta Kohl, "Eggs, Jurisdiction, and the Internet", International and Comparative Law Quarterly 51, no. 3 (2002), available at: https://doi.org/10.1093/iclq/51.3.555 (last access on 29.10.2021), 2008, p. 15.
[71] Council of Europe, "Explanatory Report to the Convention on Cybercrime", available at: https://rm.coe.int/16800cce5b (last access on 29.10.2021), 2001, Paragraph 234.
[72] Council of Europe, Explanatory Report to the Convention on Cybercrime, available at: https://rm.coe.int/16800cce5b (last accessed on 29.10.2021), 2001, Paragraph 233.
[73] Council of Europe, Explanatory Report to the Convention on Cybercrime, available at: https://rm.coe.int/16800cce5b (last accessed on29.10.2021), 2001, Paragraph 236.

double criminality requirement (both in the state of nationality and in the territory where the crime is committed) intends to ensure legal certainty. Nevertheless, it may turn out to be the perfect tool for creating the aforementioned "*safe-havens*" – for instance, in case the country where the act is committed (territoriality principle) does not criminalize a given behaviour, the nationality principle may not apply, even if that conduct is a typified crime under the laws of the country of the nationality of the perpetrator.

Both the territoriality principle, the flag principle and the active nationality principle are expressly foreseen in Art. 22 of the Budapest Convention. However, the only principle of compulsory implementation by the Signatory Parties is the territoriality principle, insofar as the Convention allows the parties not to apply the other principles [74]. The Convention further clarifies that it is mandatory to establish jurisdiction in cases falling under the principle of *aut dedere aut judicare* (extradite or prosecute), which shall be further developed bellow.

In case more than one Party has jurisdiction over some or all the participants of a given cybercrime, the Convention's Explanatory Report provides the criteria which shall apply in order to solve such a conflict[75]. More specifically, it stipulates that the affected Parties may be consulted, where appropriate, to decide on the most effective methodology, on a case-by-case basis: sometimes it may be more effective to choose a single venue for prosecution, while in other cases it may be better if some States prosecute some participants, while one or more States pursue others.

Other links worth mentioning, are those which protect pure domestic legal interests, namely, the passive personality principle and the protective principle, which are narrower versions of the principle of objective territoriality. These principles gain relevance in cases where it might be difficult to establish a purely territorial connection. In such cases, regardless of where the crime was actually committed, it may be deemed to have been committed within a given territory, as long as some other link connects the crime to that nation[76]. According to the

[74] Namely in its article 22.
[75] Namely, in its paragraph 239.
[76] Christopher L. Blakesley, "United States Jurisdiction over Extraterritorial Crime", The Journal of Criminal Law and Criminology (1973-) 73, no. 3 (1982): 1109-163, available at: https://doi.org/10.2307/1143188 (last access on 29.10.2021), 1973, p. 1119.

passive personality principle, a state defines its extraterritorial jurisdiction based on the fact that the victim is its national[77]. On the other hand, the protective principle focuses on the protection of the fundamental interests of a given state.

That said, it is important to refer that prescriptive jurisdiction is just the first step on the long ladder that leads to cybercrime enforcement. The next step is to explore whether there is any court in the competent nation, with adjudicative jurisdiction over the concrete case[78]. Finally, it is still necessary to analyse which nation has enforcement jurisdiction over that specific case. Usually, the jurisdiction which has the perpetrator in custody is the one more capable of exercising such enforcement jurisdiction[79].

The Budapest Convention foresees the possibility of extradition. However, for it to occur, the reprehensible conduct must be punishable under the laws of both countries at stake, by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty, unless a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty[80]. Basically, the convention establishes a dual criminality requirement, as well as a minimum abstract penalty threshold which further complicates the prosecution of international cybercrimes.

One important mechanism established, in this respect, in the Convention[81], is the principle "*aut dedere aut judicare*" (extradite or prosecute), according to which, if a Party has requested the extradition of the perpetrator, so that he may be prosecuted under the laws of that state, and the requested Party refuses it on the grounds of the nationality principle, it must, upon request of the other Party, submit the case to its authorities for the purpose of prosecution[82].

---

[77] Jonathan Clough, "Principles of Cybercrime, available at: https://www.cambridge.org/core/books/principles-of-cybercrime/F172001ECA8742B5C3E0678CDF977718 (last access on 29.10.2021), 2015, p. 407.

[78] *Ibidem*, p. 410.

[79] Uta Kohl, "Eggs, Jurisdiction, and the Internet", International and Comparative Law Quarterly 51, no. 3 (2002), available at: https://doi.org/10.1093/iclq/51.3.555 (last access on 29.10.2021), 2008, p. 16.

[80] Article 24 of the CoE Convention of Cybercrime.

[81] Namely, in its Article 24 (6).

[82] Council of Europe, Explanatory Report to the Convention on Cybercrime, available at: https://rm.coe.int/16800cce5b (last accessed on29.10.2021), 2001, Paragraph 233.

Overall, the transnationality of cybercrime complicates the prosecution of the respective perpetrators, mainly because states are not willing to give up on their sovereignty, even if it is for the benefit of the greater good.

Despite this, there are mutual legal assistance mechanisms, which create the basis for counties to communicate with each other, in order to solve the conflicts of interest under analysis. Such cooperation mechanisms may consist, for instance, in extradition mechanisms, treaties and arrangements for the international transfer of sentenced persons.

The Budapest Convention, namely, addresses these matters by providing mutual assistance and cooperation mechanisms.

As for international cooperation, it sets forward a general cooperation principle, according to which Parties shall cooperate with each other "*to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence*"[83]. Furthermore, it foresees the Extradition mechanism presented above. On mutual assistance, the Convention foresees the same exact general principle as provided for international cooperation. Furthermore, it provides the opportunity for Parties to communicate through expedite means (such as email) in urgent cases. It also provides the possibility for a Party to send spontaneous information to another, in case such Party believes the said information may assist the other Party in initiating or carrying out investigations or proceedings on criminal offences.

The general mutual assistance mechanism foreseen in the Convention, in its article 27, works as follows: each Party shall designate a central authority, responsible for communicating and executing mutual assistance requests; in case of an urgent request, such request shall be sent directly by the judicial authorities of the requesting Party or through Interpol, but in any other case, central authorities are the ones which shall communicate in order for an assistance request to occur; there are certain grounds on which the receptor Party may decline the request, such as in case it concerns a political offense or is likely to affect that Party's sovereignty. In parallel there are certain grounds,

[83] Article 23 of the Convention.

legally foreseen, under which a Party may postpone an assistance request. Nevertheless, before refusing or postponing mutual assistance, the Requested Party must consult with the Requesting Party, and the decision to postpone or refuse must be justified by the Requested Party.

Furthermore, the Convention includes special provisions with regard to expedited preservation of stored computer data[84], expedited disclosure of preserved traffic data[85], mutual assistance on access to stored computer data[86], trans-border access to stored computer data with consent or where publicly available[87], mutual assistance regarding the real-time collection of traffic data[88] and mutual assistance regarding the interception of content data[89]. Finally, it foresees a 24/7 Network[90] aimed at providing immediate assistance for the purpose of investigations or proceedings and for collection of evidence in electronic form on criminal offenses related to computer systems and data. Some other important cooperation Networks in this context are the 'I-24/7' system, from INTERPOL[91] and the EUROPOL's European Cybercrime Centre (EC3)[92].

Another important Convention, in this regard, is the European Convention on Mutual Assistance in Criminal Matters[93], signed by both members and non-members of the Council of Europe. Under this Convention, the Signatory Parties agree on mutual legal assistance mechanisms aimed at gathering evidence, hearing witnesses, experts and prosecuted persons.

Additionally, a legally binding document that has contributed to the development of cybercrime cooperation systems[94] is the UN Convention against Transnational

[84] Article 29 of the Convention.
[85] Article 30 of the Convention.
[86] Article 31 of the Convention.
[87] Article 32 of the Convention.
[88] Article 33 of the Convention.
[89] Article 34 of the Convention.
[90] Article 35 of the Convention.
[91] UNODC United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime", available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (last access on 29.10.2021), 2013, p.187.
[92] European Cybercrime Centre - EC3, "Combating crime in a digital age", available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (last access on 29.10.2021).
[93] Council of Europe, "European Convention on Mutual Assistance in Criminal Matters", available at: https://rm.coe.int/16800656ce (last access on 29.10.2021), 1959.
[94] United Nations Economic and Social Council (2018-2019 : New York and Geneva), "Promoting technical assistance and capacity-building to strengthen national measures and international

Organized Crime[95], which aims to "*promote cooperation to prevent and combat transnational organized crime more effectively*"[96] – a Convention of great importance, as it has been signed by 190 countries[9798].

More recent developments in the EU context include the adoption of the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters[99]. This Directive provides for the rules governing the issuance and execution of European Investigation Orders, a mechanism which may be used in order to conduct investigative measures in another Member State (than the issuing one) with the aim of gathering evidence.

The European Commission has proposed the E-evidence package that provides for the possibility for judicial orders to be addressed directly to service providers operating in the European Union[100].

Considering the overall picture exposed on this topic, it can be argued that economic operators should also play a role in these cooperation mechanisms, especially considering they are one of the most affected stakeholders in wide-scale cybercrime. Nevertheless, and as stated by the World Economic Forum, if a multinational company is the target of a cybercrime, it is still not clear which national authority should be leading the prosecuting process, or under which jurisdiction should investigations occur[101]. Aimed at addressing this unclear

---

cooperation to combat cybercrime, including information-sharing : resolution / adopted by the Economic and Social Council", available at: https://digitallibrary.un.org/record/3814466#record-files-collapse-header (last access on 29.10.2021), 2019, p. 3,4.

[95] United Nations, "Convention Against Transnational Organized Crime and the Protocols Thereto", available at: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf (last access on 29.10.2021), 2004.

[96] As provided for in its Article 1.

[97] United Nations, "Treaty Collection", available at: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en (last access on 29.10.2021), 2021.

[98] Sofia Agostinho, "Online Violations of Data Protection – The Criminal Law Perspective", Essay submitted at Nova School of Law in the context of the Course "Cybersecurity", Spring Semester 2020, p. 8.

[99] Namely in its Article 1(2).

[100] European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, available at: https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html (last access on 29.10.2021), 2020.

[101] Allison Peters & Amy Jordan, "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime", Third Way, available at: https://www.thirdway.org/report/countering-

subject, the World Economic Forum's Centre for Cybersecurity[102], the Global Forum on Cyber Expertise[103] and the EUROPOL's EC3 Advisory Group[104] were created. Each of them designed to breach the gap between the public and private sector, in order to create cooperative responses to cybercrime.

iii. Scalability and Flexibility of Decentralized Networks which Facilitate the Commission of Organized Crime

Another characteristic of cyberspace which makes it more appealing for the perpetrator is the fact that it "*allows for decentralised, flexible networks in which perpetrators can [loosely] organise themselves to divide labour or to share skills, knowledge, and tools"*[105]*.*

In this context, open-source software plays a really important role, providing free and ready to use knowledge to all interested stakeholders. Besides this, the Dark-Web also provides tempting channels, such as private anonymous chats, perpetrators may use to orchestrate crimes, recruit a new set of skills, among other procedures which may enhance the accessibility of cybercrime.

iv. The Pacing Problem[106]

The legitimacy of the law is grounded, in part, on the premise of legal certainty, achieved through the sedimentation of techniques, extended study of the subjects, and weighing of the various interests and principles involved. Such a

---

the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime (last access on 29.10.2021), 2019, p. 16.

[102] World Economic Forum, "Centre for Cybersecurity", available at: https://www.weforum.org/centre-for-cybersecurity/ (last access on 29.10.2021).

[103] FGCE, "Strengthening cyber capacity and expertise globally through international collaboration", available at: https://thegfce.org/ (last access on 29.10.2021).

[104] EUROPOL, "EC3 Partners", available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners (last access on 29.10.2021).

[105] Bert-Jaap Koops, "The Internet and its Opportunities for Cybercrime", TRANSNATIONAL CRIMINOLOGY MANUAL, M. Herzog-Evans, ed., Vol. 1, pp. 735-754, Nijmegen: WLP, 2010; Tilburg Law School Research Paper No. 09/2011. Available at: https://ssrn.com/abstract=1738223 (last access on 29.10.2021), 2011, p.740.

[106] Gary Elvin Marchant, Braden R Allenby & Joseph R Herkert, "The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem", Springer Netherlands Available at: https://www.springer.com/gp/book/9789400713550 (last access on 29.10.2021), 2011.

process evidently implies a considerable number of working hours from the various stakeholders. Additionally, in order for citizens to feel secure by the institution of law, it is of utmost importance that the law provides some stability, thus rendering it impossible to change the law every time there is an advance in the use cases for which it was created. For these reasons and in an attempt to ensure the law continues to fit the reality for as long as possible, its text is transposed to codes and individual laws in a general and abstract manner, leaving it up to the courts to adapt it to the needs of each concrete case[107].

While it is true that in most cases this mechanism works perfectly, it is also a fact that the pace at which technology evolves does not allow for the law to be permeable to technological innovations. Additionally, this pacing problem[108] is aggravated by the information asymmetries between innovators and law makers[109], hindering the gap even further. It is precisely in this context that the problem under analysis – the Pacing Problem – arises, as legislators nowadays tend to prioritize legal security over the timeliness of the law, which is why technologies such as Blockchain have yet to be regulated. However, it comes without saying that the lack of suitable rules to regulate the disruptive challenges of this modern era, provides the perpetrator with a fertile ground to grow illegal acts.

Over the years, several options have been appointed, which may help solving this problem, namely, a principle-based approach; a sector specific Common Law system; sunset clauses and experimental regulations; a guidelines-based approach; regulatory sandboxes; self-regulation; and even techno-regulation.

[107] Annika Suominen, "What Role for Legal Certainty in Criminal Law Within the Area of Freedom, Security and Justice in the EU?", Bergen Journal of Criminal Law and Criminal Justice • Volume 2, Issue 1, 2014, pp. 1-31, Available at: https://www.legal-tools.org/doc/7d0cc5/pdf/ (last access on 29.10.2021), 2014, p.6, 7.

[108] Gary Elvin Marchant, Braden R Allenby & Joseph R Herkert, "The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem", Springer Netherlands Available at: https://www.springer.com/gp/book/9789400713550 (last access on 29.10.2021), 2011.

[109] Sofia Ranchordas, "Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation" (November 1, 2014). Jurimetrics, Vol. 55, No. 2, Available at SSRN: https://ssrn.com/abstract=2544291 (last access on 29.10.2021), 2015 p. 203.

The principle-based approach provides the possibility to tackle online criminal activity through general and abstract guiding principles[110], which should then be materialized in a regulatory decision, applied by the competent stakeholder. Although this remedy may be rather flexible and suitable to keep pace with technology, one evident downside is that it leaves a lot of room for interpretation. Considering we are dealing with criminal law, which shall be the last resort to control the behaviour of citizens, leaving too much room for interpretation is not desirable, as it may lead to contradictory decisions on topics as important as the freedom of a defendant.

As for the use of a common law regime to rule the most varied cybercrimes, it seems that courts may take as long or even longer to reach a verdict than the time it would take for the law to come into effect, as such courts are often overwhelmed with cases. On the other hand, in this type of system, Courts adhere to precedent often dated from decades or centuries earlier, necessarily introducing unsuitable decisive elements to judge a conflict involving emerging technology[111].

The ruling on Microsoft antitrust case[112], is a living proof of such argument. In this case, Court *a quo* determined that Microsoft had maintained a monopoly in the market for Intelcompatible PC operating systems, attempted to gain a monopoly in the market for internet browsers, and illegally tied two purportedly separate products.

In such case, the court itself expressly states that "*What is somewhat problematic, however, is that just over six years have passed since Microsoft engaged in the first conduct plaintiffs allege to be anticompetitive."*

[110] Mark Fenwick, Wulf A. Kaal & Erik P.M Vermeulen, "Regulation Tomorrow: What Happens When Technology Is Faster Than the Law?", American University Business Law Review, Vol. 6, No. 3, 561; U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-20, Available at SSRN: https://ssrn.com/abstract=3204119 (last access on 29.10.2021), 2017, p.13.
[111] Gary Elvin Marchant, Braden R Allenby & Joseph R Herkert, "The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem", Springer Netherlands Available at: https://www.springer.com/gp/book/9789400713550 (last access on 29.10.2021), 2011, p. 24.
[112] United States of America, Appellee v. Microsoft Corporation, Appellant, 253 F.3d 34 (D.C. Cir. 2001), available at: https://law.justia.com/cases/federal/appellate-courts/F3/253/34/576095/ (last access on 29.10.2021).

The judge further develops that the period of time which occurred before the court reached its verdict – 6 years – was the equivalent to *"an eternity in computer industry*"[113], as the market tends to develop rather rapidly, complicating the judgement on the appropriate measures to apply. As for conduct remedies, these may be ineffective, since the evolution of the technology which was the object of this case has already became obsolete – hardware and software have both evolved a lot in the 6 year period which occurred, meaning that the specific products at stake no longer had a monopoly of the market

Moreover, from the compliance perspective, both economic operators and consumers would be left without any guidance or protection if the only source of law in this context was the case law, since in most cases, due to the structure of the market, it takes years for a problem to become significant enough to reach a courthouse.

Additionally, while the task forces contacted to collaborate in the drafting of laws are chosen for their technical or academic expertise in the area at stake, it is rather common to witness situations where judges currently deciding on the most innovative cases have no special training in the area or technology over which they are deciding, leaving the technical work to experts, and simply appreciating the evidence presented, and comparing it with the result from the expert's examination[114].

As for the use of sunset-clauses to tackle the Pacing Problem, one of the benefits is that they permit revoking all obsolete acts, providing a cleaner legal environment to all economic operators – if a diploma is not suitable to regulate a given subject, there is always the option to revoke it[115]. However, once again, the problem in applying this mechanism to criminal law, is that it does not provide the necessary stability that both citizens and enterprises need. Additionally, in accordance with the principle of legality, one can only punish through criminal law what is previously described and declared in legislation. On what concerns

[113] *Ibidem*.

[114] Parlamento, "Competências da Assembleia da República", available at: https://www.parlamento.pt/Parlamento (last access on 29.10.2021).

[115] Sofia Ranchordas, "Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation" (November 1, 2014). Jurimetrics, Vol. 55, No. 2, Available at SSRN: https://ssrn.com/abstract=2544291 (last access on 29.10.2021), 2015, p. 205.

experimental regulations, its phased application – they are often firstly implemented on a small-scale basis, to a compartmentalized group of individuals, and further escalated depending on the success rate of the experiment - is definitely inconsistent with the purposes and principles of criminal law, as it would discriminate citizens, providing a different level of protection in different areas.

As for the guidelines, industry standards or advisory opinions, provided by entrepreneurs and innovators themselves and by any regulatory agencies, although it leaves room for improvement and flexibility to adapt to every particular case, it is undeniable that such institute would lack on legal grounds to become a source of law, especially when such guidelines or best practices come from the private sector. For this reason, it is likely that such institutes would not have the necessary strength to be the critical factor of decision in a court of law[116].

When such guidelines come from the private sector, they may be regarded as self-regulation, because they represent the market regulating itself, as foreseen by Adam Smith, on its economic thesis[117].

Given the lack of laws in many of the technology driven branches of law, this self-regulation technique has indeed been useful, especially for the consumer, who is able to count on additional protective measures. A perfect example are the measures reported in YouTube Case law[118], where despite being an intermediary service provider whose liability statute only imposes a duty to report in case it has actual knowledge of illegal activity, the economic operator decided to impose on himself the burden of several other protective measures in the name of consumer protection and the compliance with third-party intellectual property rights[119].

---

[116] Ryan Hagemann, Jennifer Huddleston & Adam D. Thierer, "Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future", Colorado Technology Law Journal, Available at SSRN: https://ssrn.com/abstract=3118539 (last access on 29.10.2021), 2018, p. 91, 92.

[117] Adam Smith, "The Wealth of Nations", Oxford, England: Bibliomania.com Ltd, available at: https://www.loc.gov/item/2002564559/ (last access on 29.10.2021), 2002.

[118] In Joined Cases C-682/18 and C-683/18 of the CJEU, available at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=C50B2E6BBCC1BBCAD48EED6AEA3FE4DD?text=&docid=243241&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5935088 (last access on 29.10.2021), 2021, Paragraph 30.

[119] These measures include: a notification button, through which indecent or illegal content can be reported; a special alert procedure through which copyright holders are capable to have up to 10 specifically disputed videos removed from the platform by indicating the relevant internet addresses; a 'Content Verification Program' which makes it easier for the rightholder to identify

These mechanisms are really helpful even for legislators, to understand what the public is expecting and willing to give in each case. Although the enforceability of self-regulation, on its own, may definitely be challenged, as it does not emerge from a public or regulatory authority, it is, from a practical standpoint, one of the most powerful weapons to fight the pacing problem. Furthermore, the legitimacy burden could easily be surpassed in case the drafted diplomas were approved by the competent state authorities, or if the private stakeholders drafted such legal documents under the supervision of the state. This way, the time lapse between an innovative technology entering into market and its use for committing crimes would be diminished, as such documents would not have to go through the lengthy process for the approval of a law.

On what concerns Regulatory Sandboxes[120], similar to sunset clauses, it is not the most adequate tool to address cybercrime, as it would be quite paradoxical to permit testing criminal conducts, since there are legal goods at stake.

Finally, on what concerns techno-regulation (i.e., the technology regulating itself through the use of technical and organizational measures, which is the case, for instance, of the measures implemented by Netflix, which prohibit users from downloading the platform's content), even though it is definitely useful in an online environment, it may never be regarded as a source of law. Additionally, more often than not, it is difficult to implement the appropriate technical measures to prevent data related cybercrimes from happening, directly from the source.

Another innovative method for solving the pacing problem is the use of direct final rulemaking, a variation to the traditional rulemaking process, where the legislator issues the diploma without going through public comment, with reference that unless it receives any adverse comment or written notice, it will become

the videos that he or she considers to infringe his or her rights by checking them off in a list of videos; a content-recognition software to identify illegal content; among others.

[120] Dirk Andreas Zetzsche, Ross P. Buckley, Douglas W. Arner & Janos Nathan Barberis, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation", 23 Fordham Journal of Corporate and Financial Law 31-103 (2017), European Banking Institute Working Paper Series 2017 - No. 11, University of Luxembourg Law Working Paper No. 006/2017, University of Hong Kong Faculty of Law Research Paper No. 2017/019, UNSW Law Research Paper No. 17-71, Center for Business and Corporate Law (CBC) Working Paper Series 001/2017, Available at: https://ssrn.com/abstract=3018534 (last access on 29.10.2021), 2017, p. 25.

effective[121]. In case the diploma receives substantial adverse comments, it will be withdrawn and sent to the proper traditional channels for further analysis. When applied to data related cybercrimes, direct final rulemaking may be helpful to the extent it is used to tackle problems with rather consensual solutions, which implies there has to already be some pre-existing opinions on the subject. Considering we are at a stage where the topics are still not studied enough to have a substantiated consensus, such a mechanism may be, for now, of little use, if the goal is to address online violations of data protection.

Overall, there seem to be quite a few useful alternatives for regulating technology. Without prejudice, even if legislation is not the optimal solution to regulate data related crimes, if this approach is maintained by the legislator, there is an urgent need to create a data protection code, capable of organizing the various dispersed laws.

[121] Ronald M. Levin, "Direct Final Rulemaking", George Washington Law 64: 1–34, available at: https://www.acus.gov/sites/default/files/documents/1995-04%20Pt.2%20Procedures%20for%20Noncontroversial%20and%20Expedited%20Rulemaking.pdf (last access on 29.10.2021), 1995, p. 1, 2.

III. PRIVACY-RELATED CRIMES COMMITTED ONLINE

a. What is Data After All?

Personal data is defined in the GDPR. However, the legislator focused on defining the personal element, leaving the definition of data to the academia. While personal data refers to any information relating to an identified or identifiable natural person, "*non-personal data represents data which personal information cannot be derived from*"[122].

Ackoff represents data as symbols. Information, on the other hand consists of processed data. Such processing aims at increasing the usefulness of data, while still representing objects and events. In this context, the author pertinently refers that the difference between information and data is functional, not structural[123]. Basically, data represents non-interpreted information.

Data are non-corporeal goods, where there is no scarcity, hence it may be replicated as many times as the data subject wishes. Data can be accessed. In that context, it is possible to analogically link access to possession- while possessing a corporeal good provides the possessor with the possibility to use such good as he pleases (within the limits that may have been established by the owner of such good), the one with access to data may use such data for the purposes (s)he deems convenient [124]-, even though the person who accesses the data does not necessarily have it in his physical possession. Of particular interest are the solutions considering data as property, aiming at providing citizens with a certain level of ownership and control over their data.

[122] Ivan Stepanov, "Introducing a property right over data in the EU: the data producer's right – an evaluation", International Review of Law, Computers & Technology, 34:1, 65-86, available at: https://www.tandfonline.com/doi/pdf/10.1080/13600869.2019.1631621?needAccess=true (last access on 29.10.2021), 2020, p. 67.
[123] Russell Ackoff., "From Data to Wisdom." In Ackoff's Best, 170–172. New York: John Wiely and Sons, available at: https://faculty.ung.edu/kmelton/Documents/DataWisdom.pdf (last access on 29.10.2021), 1999, p. 1.
[124] Herbert Zech, "Information as Property", 6 (2015) JIPITEC 192, available at: https://www.jipitec.eu/issues/jipitec-6-3-2015/4315/zech%206%20(3).pdf (last access on 29.10.2021), 2015, p. 195.

Lessig[125] argues that property rules would allow citizens to choose which information to share. Additionally, given the structure of cyberspace, this solution provides the data users with the unique opportunity to truly determine who has access and control over their data, as they would be the only ones in a position to transmit it - because as our ancestors stipulated, *nemo plus juris transferre potest quam ipse habet.* For such property right to exist, it would have to be provided for in a given legal system, as there is a limited number of property rights. According to Lessig, the current regime on data protection foresees the opposite, i.e., a liability rule ensuring transfers of data are possible, but the data subject shall be compensated if such a transfer, access, use or any other data processing is conducted unlawfully. On the other hand, if data were protected by a property rule, it would not be stripped from the data subject, unless voluntarily transmitted by him (as he would be the only one entitled to transmit it)[126].

The main difference between these two approaches is in fact that the property regime nips the evil in the bud, making it impossible for the offender to impose himself or herself on someone else's property in the first place. In case there was a property right over data, this should be, *a priori*, non-transferable, to protect the data subject from losing the rights over his own personal data. Still, the data subject would be able to grant the usufruct of his data to whom he wished.

Usufruct is a minor *in rem* right, meaning a right that coexists with the property right, limiting the rights of the proprietor. In the Portuguese legal system, for instance, it is possible to have multiple simultaneous usufructs over the same good[127] (in this case, there is a joint usufruct for the same period of time) or successive usufructs (where the second usufruct only begins when the first one ends)[128].

---

[125] Laurence Lessig, "Code and Other Laws of Cyberspace", New York, Basic Books, available at: https://dl.acm.org/doi/10.5555/555000 (last access on 29.10.2021), 1999.
[126] Nadezda Purtova, "Property in Personal Data: a European Perspective on the Instrumentalist Theory of Propertisation", European Journal of Legal Studies, 2010, 2, 3, The Future of Law & Technology in the Information Society, available at: https://core.ac.uk/download/pdf/45678038.pdf (last access on 29.10.2021), 2010, p. 11.
[127] As provided for in Article 1441 of the Portuguese Civil Code.
[128] Pº C.P. 11/2004 DSJ-CT., "Usufruto simultâneo e sucessivo", available at: https://www.irn.mj.pt/IRN/sections/irn/doutrina/pareceres/predial/2004/p-c-p-11-2004-dsj-ct/downloadFile/file/pcp011-2004.pdf?nocache=1315923809.68 (last access on 29.10.2021) , p. 5.

A conceptual characteristic of property rights all over Europe, is that they are *erga omnes* rights, i.e., rights which impose themselves to all third parties. According to Stepanov, transparency is an imperative requirement for a right to qualify itself as an *erga omnes* right, namely, third parties must be given the opportunity to get acquainted with such property right[129]. He considers such acquaintance to be practically impossible under existing market practice, hence, the author argues property over data must be conferred under the form of a new intellectual property right introduced by the European Commission in 2017[130], namely, the "*data producer's right*".

Nevertheless, as personal data are intrinsically linked to the person to whom they belong, its receiver would not have to verify whether it belongs to the transmitting party. What he would have to check is whether the usufruct right which was transmitted accounted for the possibility of the usufructuary transmitting the data to third parties.

A hypothetical scenario is that of a user granting a platform the right of usufruct over his email address in exchange for a service provision by allowing it not only to use his email address to send a weekly advertising newsletter, but also to transmit the right directly granted by the user to third parties.

When an advertising company receives a contractual proposal from a platform, under which the platform commits to share that user's email address with the advertising company, what the latter would have to check was not whether the personal data belonged to the platform, since obviously it would not (as it would not be possible to transfer the property, but merely to grant an usufruct right over such data). Instead, the advertising company would have to check whether the contract under which the usufruct was established, foresees the possibility for the platform to transmit the right to third parties, and if so, whether the contractually

[129] Ivan Stepanov, "Introducing a property right over data in the EU: the data producer's right – an evaluation", International Review of Law, Computers & Technology, 34:1, 65-86, available at: https://www.tandfonline.com/doi/pdf/10.1080/13600869.2019.1631621?needAccess=true (last access on 29.10.2021), 2020, p.70.

[130] European Commission, "Communication on Building a European Data Economy", available at: https://digital-strategy.ec.europa.eu/en/library/communication-building-european-data-economy (last access on 29.10.2021), 2017, p. 13.

established requirements are met. This way, the transparency requirement would be met.

Notwithstanding, it is worth analysing the European Commission's Communication on Building a European Data Economy. The Commission issued a statement on the various possibilities for addressing the issue of access to machine-generated data, among which was the data producer's right – "*A right to use and* authorise the use of non-personal data could be granted to the "data producer", i.e., the owner or long-term user (i.e. the lessee) of the device"[131]. The purpose of this right would be to increase data sharing by providing the data holder (and not the data subject) with certain defensive elements of an *in rem* right, namely, the capacity to sue third parties for illicit misappropriation, protecting possession instead of ownership. This right would cover "*the right to seek injunctions preventing further use of data by third parties who have no right to use the data, the right to have products built on the basis of misappropriated data excluded from market commercialisation and the possibility to claim damages for unauthorised use of data*"[132].

This proposal/concept is based on the fact that information may be dissected into several layers: the semantic layer representing understandable or meaningful information to the human eye; a syntactic layer, which stands for information represented by a certain code; and the physical layer, which stands for information in its most raw form, contained in a given physical carrier[133]. This right was meant to protect non-personal or anonymized data and metadata at the syntactic level, generated by a machine as an economic good. Hence, it does not protect any ideas or information.

Another approach suggested by the European Commission to ensure companies are properly remunerated by third parties' use of their non-personal or anonymized data is a liability-based regime. As explained above, such regime

---

[131] *Ibidem*.

[132] European Commission, "Commission Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002&from=EN (last access on 29.10.2021), 2017, p.33, 34.

[133] Herbert Zech, "Information as Property", 6 (2015) JIPITEC 192, available at: https://www.jipitec.eu/issues/jipitec-6-3-2015/4315/zech%206%20(3).pdf (last access on 29.10.2021), 2015, p. 194.

protects against unlawful use, where similar to the regime foreseen in the Trade Secrets Protection Directive, protection grant would depend on the technical protection efforts adopted by the data holder.

Overall, the best-case scenario would be the one where the data subject is given the right to property over his personal data (even if not transferable) and is able to create a usufruct in favour of whom he wishes. However, entities with lawful access to or possession of data, who render it into non-personal or anonymized data, should also benefit from some protection. In this case, the data producer's right seems like the best fit. As for the concept of data as a commodity, the EU has already stated that such approach is not desirable[134], especially since it would lead to a scenario where those less wealthy would sell their data more easily.

b. Old Wine New Bottles or New Bottles Old Wine?

To some extent, and as mentioned above, most crimes committed online can be regarded as a variation of an existing well established offline crime. For instance, data breaches can, to some extent, be considered a theft, as they were both conceived to prevent unauthorized intrusions over proprietary content, even if in one case, the legal good protected is privacy and in the other, is property. However, in this context, there is a huge difference, since as explained above there is no scarcity in data, which means that when an offender misappropriates the data, he may merely replicate it, which means there is no subtraction of a proprietary element.

In parallel, identity theft could be regarded as a forgery. However, the act of stealing as typified in most criminal codes, is related to material goods, and as mentioned above, data is a non-corporeal good.

[134] As provided for in Recital 24 of Directive 2019/770 of the European Parliament and of the Council of 20 May 2019, on certain aspects concerning contracts for the supply of digital content and digital services, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0770&from=EN (last access on 29.10.2021) – "While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies".

If legislators had chosen to simply include these new variations of crime, in the already existing types of crime the aforementioned specific elements of cybercrime, would arise, one by one, in all concrete problems, making it really difficult to prosecute the perpetrator.

Another possible approach would have been to simply alter the existing laws, altering the provision that criminalizes theft, so that it includes illicit or non-consented access data. However, generally speaking, neither substantive nor procedural criminal law were ready to deal with cybercrime.

In order to properly illustrate how this dynamics would not be the most suitable one, an example may be helpful. For instance, the Portuguese national provision which criminalizes theft applies to anyone who "*with illegitimate intent to appropriate for himself or another person, subtracts another's movable property*"[135]. In case such provision was meant to apply to data breaches as well, a problem would arise from the fact that the data, while not having a well-defined legal qualification (as illustrated above), is definitely not susceptible to "*subtraction*" in the sense intended by the expression set forth in the Portuguese Criminal Code, insofar as there is no scarcity of the data. By illegitimately using or accessing other people's personal data, the criminal is not removing the possession or ownership of such data from the sphere of its holder.

In the author's perspective, merely altering the existing laws would not be the most suitable approach, not only for the already exposed reasons, but also because, cybercrime has its own needs. For instance, it would not be conceivable that the same policeman who acts upon theft, would be in charge of cybercrime as well. Cybercrime needs its own specialized policemen, as well as its own mutual assistance and cooperation mechanisms.

As already (at least partially) explained above, the CoE Cybercrime Convention plays an important role in this field, providing a set of cybercrimes, ensuring a minimum level of harmonization among its Signatory Parties and achieving an efficient mutual assistance mechanism. Of utmost importance is that such

[135] Article 203 of the Portuguese National Criminal Code.

Convention adopts a technology neutral approach, in order to account for upcoming types of crime or new ways to commit the existing ones.

Other relevant legal instruments are Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, Directive 2002/58/EC[136] of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, the GDPR, and Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems (hereinafter also referred to as "*Directive*") and replacing Council Framework Decision 2005/222/JHA.

Our purpose on the next chapters is indeed, to analyse the respective legal provisions that contemplate online violations of data protection, in which the protected legal good is the victim's privacy.

In the next subchapters proper notice will be granted to some of the current typified data related crimes, which aim to protect the legal good of privacy, illustrating the techniques adopted by the legislator of the CoE Convention (which is not a mere EU legal instrument, but rather an international one) and of European Union Directives.

i. Illegal access

This criminal offence aims to protect the confidentiality, integrity and availability of computer systems or data and therefore, people's safety and privacy.

In accordance with the CoE Convention, for the perpetrator to commit it, he must intentionally access a computer system, without right, so basically the crime must

[136] Amended by Directive 2006/24/EC and complemented by Regulation (EU) No 611/2013. This Directive should have been repealed by Regulation of The European Parliament And Of The Council, concerning the respect for private life and the protection of personal data in electronic communications, by January 2018- ePrivacy Regulation. Following the failure of the latest draft, commentators do not expect the ePrivacy Regulation to enter into force before 2023. At this point, there is also the prospect that the European Commission will withdraw the draft legislation completely, leaving a lot of data protection problems with no legal response.

be conducted by an agent or organization which gains unauthorized and intentional access to a computer system.

The intent criterion has the purpose of excluding from the scope of the Article, conducts which are not serious enough to be ruled by criminal law. However, in a criminal context, proving the intention to commit a crime before a court is not always a straightforward exercise. Only the criminal knows his intention at the time of committing the illicit act. Thus, proof of intent is no more than a fictitious reconstruction of what the perpetrator intended and is therefore subject to the rule of the best argument presented. Consequently, requiring that the perpetrator acts with the intention to access computer systems without authorization may not be the best fit for a branch of law which has already got so many layers of complexity.

While the reconstruction of the agent's intention must always be based on a fictitious creation of what the agent might think before or at the time of committing the crime, other criteria such as the impact of the conduct or its qualification as organized crime (which are usually addressed, in legal criminal documents, as aggravations circumstances) are, in the opinion of the author, more objective, largely facilitating judicial authorities' work.

Additionally, these criteria would help criminalize only those conducts of illegal access that are indeed serious enough to be addressed by criminal law.

Furthermore, the Convention provides each signatory Party with the possibility to "*require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent*"[137].

Such requirement makes it very likely for an act of illegal access to materialize into another type of crime, making the pertinence of criminalizing such behaviour questionable, since the same result could have been achieved by giving the ratifying Parties the possibility to criminalize the attempt to commit any of the other types of data related crimes foreseen in the Convention - a less intrusive solution which is actually established in the Convention, and is applicable to all

[137] As provided in Article 2 of the CoE Convention.

crimes therein, with the exception of illegal access, a choice that, in the author's perspective, was not the most appropriate.

Nevertheless, there are still some cases where the mere illegal access, without any further additional act, may cause some serious damage to the victim, especially when dealing with sensitive or confidential data, such as, for instance, illegal access from an insurance company to the medical records of its clients.

When applied to the offline world, illegal access is comparable to illegal trespassing of private property. Similar to what happens in the online world, the commission of this crime differs in impact, depending on the characteristics of the property you are accessing – it will always be more reprehensible if a person illegally enters into an occupied house than into a non-occupied farm, even if the goal of such access is merely to prove one's capability of trespassing the security barriers.

Another argument which can be used against criminalization of illegal access, is that it further complicates the conduction of tests to identify vulnerabilities of computer systems, which may be an obstacle for early-stage software development process[138].

On another note, still on the topic of illicit access, it is relevant to analyse what should be considered, nowadays, a computer system.

In this context, CoE Convention's Explanatory Report clarifies that a computer system shall be any "*device consisting of hardware and software developed for automatic processing of digital data"*[139]*.* Once again, the legislator adopted a technologically neutral approach, hence, many gadgets which did not exist at when the Convention came into force, still fall under its scope. Some examples are, for instance, most interoperable devices, such as smart watches or smart tvs[140]. Thus, should such devices be accessed without right, it is likely they will be the object of an illegal access crime.

[138] Aleš Završnik, "Towards an Overregulated Cyberspace – Criminal Law Perspective." Masaryk University journal of law and technology 4: 173-190, available at: https://journals.muni.cz/mujlt/article/view/2566 (last access on 29.10.2021), 2010, p.182.
[139] Namely, in its recital 23.
[140] Ionita Gheorghe Iulian, "Trends and Developments in Use and Implementation of Cybercrime Convention", 2015 Conf. Int'l Dr. 870, available at:

The confirmation of the latter affirmation is provided by the Council of Europe, in its Guidance Notes, where it expressly states that the definition of computer system accounts for "*developing forms of technology*"[141], a statement rather useless, as one would reach the same conclusion in case it did not exist. This is due to the fact that Recital 36 of the Convention's Explanatory Report mentions that the Convention is technologically neutral, in order to cover not only existing technologies, but also those that may emerge during its validity[142].

As for the use cases of this type of crime, it is pertinent to refer that the use of unauthorized spyware tools usually may fall into the scope of illegal access.

Another very common use case is where websites use unauthorized cookies to monitor browser patterns. Unauthorized access may consist, for instance, in those cases where the user does not expressly consent to the use of cookies.

In this context, the CoE Convention's Explanatory Report mentions, in its recital 48 that the application of "*cookies to locate and retrieve information on behalf of communication*" may result in an illegal access for the purposes of the Convention. The application of such tools *per se* is not "without right", further explaining that the authorization in this case depends on the user's consent.

A realistic use case of such cybercrime is Operation Mousetrap, named by the Europol's European Cybercrime Centre (hereinafter EC3), where EU citizens are suspected of using remote access trojans (RATs) to commit cybercrimes. As defined by the Europol, in its website, "*Remote access Trojans are malware that are used to spy on victims' computers",* accessing all kinds of personal data, including through the recording of the user's actions when browsing the web, its webcam and microphone produced data[143].

---

https://heinonline.org/HOL/LandingPage?handle=hein.journals/cidstue2015&div=116&id=&page = (last access on 29.10.2021), 2015, p. 871.

[141] Council of Europe, "T-CY GUIDANCES NOTES Adopted by the 8th and 9th Plenaries of the T-C", available at: https://rm.coe.int/16802e7132 (last access on 29.10.2021), 2013, p. 5.

[142] Ionita Gheorghe Iulian, "Trends and Developments in Use and Implementation of Cybercrime Convention", 2015 Conf. Int'l Dr. 870, available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/cidstue2015&div=116&id=&page = (last access on 29.10.2021), 2015, p. 870.

[143] EUROPOL, "Users of Remote Access Trojans Arrested in EU Cybercrime Operation", available at: https://www.europol.europa.eu/newsroom/news/users-of-remote-access-trojans-arrested-in-eu-cybercrime-operation (last access on 29.10.2021), 2014.

ii. Illegal interception

Another crime typified in the CoE Convention is Illegal Interception[144], which aims to protect the right to privacy of data communication.

This provision consists of the intentional interception, by technical means and without right, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Once again, the possibility for the signatory parties to require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system, is foreseen in the CoE Convention.

According to the Convention's Explanatory Report[145], Interception "*by technical means*" refers to "*listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices*", among others.

As for the "*non-public*" part, the Convention's Explanatory Report clarifies that the term refers to the transmission and not the data itself. Hence, for a conduct to fall within the scope of the type of crime, the data which is shared as a topic of conversation may be publicly available, as long as the communication itself, (i.e., the transmission of that data), is not.

Most multilateral cybercrime conventions limit the object of this offence to "*non-public transmission of computer data*", as is the case of the CoE Convention (in its Article 3), in an attempt to promote confidentiality in private communications, however, on the national level, some countries opt for a wider scope[146].

[144] Namely, in its Article 3.
[145] Namely, in its Recital 53.
[146] UNODC United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime", available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (last access on 29.10.2021), 2013, p. 86.

Regarding the concept of transmission, it is pertinent to ask whether the status of "*transmission*" only includes the period before the system of destination is reached, or alternatively, whether the transmission period should include the period where the data is already stored in the system, but the recipient has not yet accessed it. No multilateral instrument provides guidance on the endpoint of transmission[147], leaving it for the signatory Parties to decide it through national legislation, which once again, may compromise unification.

Considering that the punishment illegal interception aims at protecting the privacy of data communications, it is important to clarify what is or is not a communication, especially since neither the Convention nor the EU Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems clarify this definition.

It is clear that, for instance, a message sent from one computer system to another, which contains a reply to a social media conversation, is definitely a communication. However, is the traffic data necessary for a given procedure, which might or might not be the transmission of a message from one individual to another, be considered a communication? Traffic data, as defined by the CoE Convention, means "*any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service*". Examples of traffic data in an offline context are the address and return address, the stamp and the postmark. Examples of traffic data in an online context are an URL or search term, an email or an IP address. Even though this information merely represents binary instructions, it may be regarded as personal data as it may lead to the identification of a given person[148]. In this context, should traffic data be regarded a communication and consequently, should its illegal interception fall into the scope of the crime under analysis?

[147] Ibidem, p. 87.

[148] Jonathan Clough, "Principles of Cybercrime, available at: https://www.cambridge.org/core/books/principles-of-cybercrime/F172001ECA8742B5C3E0678CDF977718 (last access on 29.10.2021), 2015, p. 153, 154.

The classification of certain data or information as traffic data or as the content of a given communication should be examined on a case-by-case basis, and the differing element should be whether the information provided by traffic data may reveal substantial or meaningful parts of a communication. Additionally, whether or not traffic data is deemed, in a given case, as personal data, might also be relevant – for instance, if a given user types his medical condition in a search engine, this information should be regarded as a communication, in order to give such user the relevant protection under the illegal interception crime.

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter "*Directive on privacy and electronic communications*") also addresses the issues at stake, namely in article 5, stating that "*Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so*".

iii. Data Interference and System Interference

Data interference, is also criminalized under the CoE Convention. It addresses the act of intentionally damaging, deleting, deteriorating, altering or suppressing computer data without right.

Damaging and deteriorating relate to a negative alteration of the integrity or of information content of data programmes. Deletion, on the other hand, represents the destruction of the data. Suppression stands for any action that prevents or terminates the availability of the data, and alteration means simply the modification of the data[149].

[149] Council of Europe, "Explanatory Report to the Convention on Cybercrime", available at: https://rm.coe.int/16800cce5b (last access on 29.10.2021), 2001, Paragraph 61.

According to the CoE Convention's Explanatory Report, this provision aims at conceding computer data and programs the same level of protection that is conferred to corporeal objects. In this context, it is also pertinent to refer that it aims at protecting "*the integrity and the proper functioning or use of stored computer data or computer programs*"[150].

Also foreseen in the Convention, the crime of system interference refers to the intentional serious hindering of the functioning of a computer system by imputing, transmitting, damaging, deleting, deteriorating, altering or supressing computer data, without right, and aims to protect the proper functioning of computer or telecommunication systems operated by a given user[151].

In this case, the term "*hindering*" stands for all actions that may interfere with the proper functioning of a given computer system, such actions must be serious, a criterion which shall be determined individually by each party.

In Accordance with the CoE Convention's Explanatory Report, examples of attacks which may be deemed as serious are those executed by programs capable of generating DoS attacks, malicious codes or programs which send a lot of email messages to a given person, in order to block the system[152].

Malicious code, also known as malware, is a term used to refer to "*a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than the intended by their owners*"[153]. It encompasses, for instance, viruses, worms and torjans, intrusions covered by the Convention, which can amount to several crimes, such as data interference and system interference[154].

In this context, it might be pertinent to ask to which extent a given system interference will not be considered a data interference as well. If data has been

[150] Council of Europe, "Explanatory Report to the Convention on Cybercrime", available at: https://rm.coe.int/16800cce5b (last access on 29.10.2021), 2001, Paragraph 60.
[151] Ibidem, Paragraph 65.
[152] Ibidem, Paragraph 66, 67.
[153] OECD, "Computer Viruses and Other Malicious Software: A Threat to the Internet Economy", OECD Publishing, Paris, available at: https://doi.org/10.1787/9789264056510-en, (last access on 29.10.2021), 2009, p. 21.
[154] Council of Europe, "T-CY Guidance Note #7 – New forms of Malware - Adopted by the 9th Plenary of the T-C", available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e70b4 (last access on 29.10.2021), 2013, p. 3.

retrieved from a computer, it is obvious that not only the data has been tempered with, but also the system, since to get to such data, the perpetrator would necessarily have to hinder the computer system. As a matter of fact, one of the necessary elements of the system interference type of crime is that data is inputted, transmitted, damaged, deleted, deteriorated, altered or suppressed. Hence, the commission of one of these crimes, will imply the commission of the other, leaving some doubts as to whether they were considered separately in the first place.

A real-life example of a system interference that ultimately resulted in a data interference is the so-called Operation Rubly[155]: A botnet was used by a large number of perpetrators to gain remote access and control over third party computers (system interference and / or illegal access), allowing them to steal personal data (including banking information) and to disable antivirus protection (data Interference).

However, even though to commit data interference it is frequently (if not always) necessary to commit system interference, the opposite is not always true, as there may very well be some attacks where the perpetrator merely denies the victim's access to the data in a given device, but for that, he will not have to necessarily temper with the data. This may happen in some DoS attacks[156], which are those where the perpetrator renders the computer system unavailable to its user and in some cases, through this process, ends up tempering with the computer data. Another use case are the Distributed Denial of Service Attacks, which represent denial of service attacks conducted by a series of coordinated computers[157].

Another very typical case which may be subsumed under the data interference crime is that of ransomware attacks, where a malicious code encrypts the

[155]EUROPOL, "Botnet Taken Down Through International Law Enforcement Cooperation", available at: https://www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation (last access on 29.10.2021), 2015.
[156] Jonathan Clough, "Principles of Cybercrime, available at: https://www.cambridge.org/core/books/principles-of-cybercrime/F172001ECA8742B5C3E0678CDF977718 (last access on 29.10.2021), 2015, p.101, 102.
[157] Council of Europe, "T-CY GUIDANCES NOTES Adopted by the 8th and 9th Plenaries of the T-C", available at: https://rm.coe.int/16802e7132 (last access on 29.10.2021), 2013, p. 9.

personal data, and subsequently the attacker asks for a ransom in exchange for the decryption code[158]. An example of a ransomware attack was the so-called CryptoLocker Operation[159], where malicious code was used to encrypt all files of the victim's computer, extorting an amount of USD 750 or more to receive the password necessary to unlock the files.

The use torjan horses and viruses is also classified as data interception, as they represent the modification of existing data[160].

iv. Misuse of Devices

The Budapest Convention[161] criminalizes the misuse of devices for the purposes of committing the aforementioned crimes. Namely, in accordance with the Convention, "*Each signatory Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences*" the intentionally and without right "*production, sale, procurement for use, import, distribution or otherwise making available of: a device including a computer program, designed or adapted primarily for the purpose of committing any*" of the aforementioned offences, or "*a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it will be used for the purpose of committing any of the*" aforementioned offences. Additionally, the possession of one of the items referred above, "*with intent that it be used for the purpose of committing"* any of the aforementioned offences, shall also be criminalized under the signatory parties domestic laws.

[158] EDPB, Guidelines 01/2021 on Examples regarding Data Breach Notification, available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en, 2021, pp. 7.
[159] EUROPOL, "International Action Against 'Gameover Zeus' Botnet And 'Cryptolocker' Ransomware", available at: https://www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware (last access on 29.10.2021), 2014.
[160] Council of Europe, "Explanatory Report to the Convention on Cybercrime", available at: https://rm.coe.int/16800cce5b (last access on 29.10.2021), 2001, Paragraph 61.
[161] Namely, in its Article 6 (1).

Distribution represents the act of forwarding data to others and making available stands for placing online devices for the use of others or hyperlinks to ease access to such devices[162].

In Article 6 of the Convention, the element of intent is referred twice. Just like in the case of the other crimes codified in the Convention, the misuse of devices has to be committed intentionally. Furthermore, the perpetrator must have the direct intention to use the device and/or access data for committing one of the illicit acts mentioned above[163].

The Convention allows its signatory Parties to abstain from criminalizing the production or import of the devices under analysis.

Neither the Convention nor its explanatory report provide a definition of the term "*device*". It can be argued that such void is intentional, so that the type of crime remains technologically neutral, in order to fit the biggest number of cases possible, as well as to ensure that it does not become obsolete. Nevertheless, it has also been argued that the concept was drawn to encompass both hardware and software[164].

The purpose of Article 6 of the Convention under analysis is to prevent the creation of black markets for the use and sale of these devices or access data, which can be used to facilitate the commission of the aforementioned illegal activities. Basically, with this provision, the legislator aimed to hinder access to the tools and means necessary to commit illegal acts.

One of the current applications of this article is to prohibit the production, sale, procurement for use, import, distribution or otherwise making available, as well as the possession of devices such as botnets or programmes used for their creation or operation[165].

---

[162] Council of Europe, "Explanatory Report to the Convention on Cybercrime", available at: https://rm.coe.int/16800cce5b (last access on 29.10.2021), 2001, Paragraph 72.
[163] Council of Europe, "Explanatory Report to the Convention on Cybercrime", available at: https://rm.coe.int/16800cce5b (last access on 29.10.2021), 2001, Paragraph 76.
[164] Jonathan Clough, "Principles of Cybercrime, available at: https://www.cambridge.org/core/books/principles-of-cybercrime/F172001ECA8742B5C3E0678CDF977718 (last access on 29.10.2021), 2015, p. 101, 102.
[165] Council of Europe, "Cybercrime Convention Committee T-YC Guidance Note #2, on Provisions of the Budapest Convention covering botnets", available at:

On what concerns the dual-use devices, they are purposely not mentioned in the Convention. Such an approach was aimed at covering as many situations as possible, eliminating the cases in which the devices are not acquired or used for illegal purposes, through the establishment of the intent requirement, which has already been analysed above[166].

As the exposition on the crimes typified under the Budapest Convention ends in the present sub-chapter, the author deems pertinent to mention the crime of identity theft, which is the perfect use case of all the cybercrimes referred so far.

Such crime represents the cases where the identity of a data subject is unlawfully used, without the data subject's consent[167].

In this regard, the Council of Europe clarifies that depending on the outlines of each specific case, identity theft may fall into the scope of several cybercrimes foreseen in the convention, among which the author highlights illegal access and interception, data and system interference, as well as misuse of devices[168].

As for the illegal access, it may be committed in cases where, in order to gain access to the data subject's identity, the perpetrator enters into his computer system, without right. Furthermore, if the perpetrator decides to intercept private communications, in order to unveil the data subject's personal data, he may be committing illegal interception. In the process of intercepting the computer data, the cybercriminal may damage computer data and hinder the function of the computer system. This may be the case, when the offender cannot find the victim's identity data in his personal communications and consequently decides to install a malicious code capable of damaging files and vital system settings. In such a case, he may also be prosecuted for committing data and/or system interference. Finally, another possible scenario is the one where a cybercriminal offers for sale an access code capable of providing the purchaser with access to

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7094 (last access on 29.10.2021), 2013, p. 4.

[166] Council of Europe, "Explanatory Report to the Convention on Cybercrime", available at: https://rm.coe.int/16800cce5b (last access on 29.10.2021), 2001, Paragraph 73.

[167] Bert-Jaap Koops & Ronald Leenes, Datenschutz und Datensicherheit 2006 (9), pp. 553-556., available at: https://www.researchgate.net/publication/228199147_ID_Theft_ID_Fraud_andor_ID-Related_Crime_-_Definitions_Matter (last access on 29.10.2021), 2006, p. 6.

[168] Council of Europe, "T-CY GUIDANCES NOTES Adopted by the 8th and 9th Plenaries of the T-C", available at: https://rm.coe.int/16802e7132 (last access on 29.10.2021), 2013, p. 13.

the computer system where the data user's credentials are stored. In such a case, the offender may be committing the crime of misuse of device.

When faced with a scenario, as the one analysed above, one might ask, what is the Convention's response to the cases where a single conduct may fall in the scope of several types of crime? As the convention does not solve this dilemma, it can be assumed that the decision should be left to each signatory Party. In this regard, Portugal, for example, consecrates as a solution, within its national Criminal Code, the punishment of the agent only for the most aggravated crime in cases in which there is a consummation relationship such as the one exposed herein[169].

v. Data Breach

The GDPR imposes on controllers and processors the need to establish the proper organizational and security measures. Should such security measures fail and a data breach occur, the controller will mandatorily need to report such data breach to the respective supervisory authority, in case such data breach is likely to result in a high risk to the rights and freedoms of natural persons[170].

Under the terms of the GDPR, 'personal data breach' means a "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*"[171].

In this context, "*destruction*" stands for situations where the "*data no longer exists, or no longer exists in a form that is of any use to the controller"; "damage*" refers to "*personal data which has been altered, corrupted, or is no longer complete*"; "loss" relates to the cases where "*the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession*"; and "*unauthorized or unlawful processing*" may include the "*disclosure of personal data to (or access*

[169] Jorge de Figueiredo Dias, "Direito Penal Parte Geral Tomo I – Questões Fundamentais a Doutrina Geral do Crime", Gestlegal 3rd Edition, available at: https://www.almedina.net/direito-penal-parte-geral-tomo-i-1574259663.html (last access on 29.10.2021), 2017, p. 1202-1205.
[170] Article 34 of the GDPR.
[171] Article 4(12) of the GDPR.

by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR"[172].

In order to incur on a data breach, it is likely that one of the aforementioned cybercrimes is committed – for instance a data breach is likely to imply incurring in an illegal access or data interference crime. In this context, it is relevant to question the pertinence of approaching the right to privacy both from a civil and criminal law standpoint, namely through the criminalization of the aforementioned crimes in the Convention (as for the criminal approach), and the use of administrative and civil penalties in the GDPR (as for the civil approach and eventually also criminal approach, in case a given Member State chooses to impose criminal sanctions for non-compliance with the GDPR, since the Regulation itself does not introduce criminal liability per se, but merely provides the option for Member States to do so).

One argument which may justify such a choice is that in case we did not have this statutory overlap, the cases which do not fall under the scope of criminal law (for instance, because they are minor both in nature and impact), would be left unpunished. For example, if the data controller incurs in a data breach due to a minimal technological mistake by one of its IT employees, since most jurisdictions do not criminalize negligent data protection violations, the conduct of the employee may not be regarded as a cybercrime.

Additionally, for those cases where the impact of the act is minor and national legislations stipulate the impact of the conduct as a requirement for the crime at stake to be committed, if the GDPR had not foreseen the proper civil sanctions, such conducts would go unpunished and it is also likely that the victim would not be informed of how vulnerable his/her data is.

On the other hand, considering that, most jurisdictions do not classify data related cybercrimes as public crimes, and economic operators will suffer a broader economic and image damage for reporting a cybercrime to the competent authorities, their motivation to report these crimes is almost inexistent. With the

[172] Article 29 Data Protection Working Party, "Guidelines on Personal data breach notification under Regulation 2016/679 (WP250rev.01)", available at: https://ec.europa.eu/newsroom/article29/items/612052 (last access on 29.10.2021), 2017, p.7.

GDPR's obligation to report data breaches which may result in a high risk to the rights and freedoms of natural persons, the data controller cannot hide the vulnerability ha may have suffered from, increasing the level of security for users and data subjects, and facilitating the work of law enforcement agencies.

In sum, the GDPR is the perfect complement to the criminal laws addressing reprehensible data related conducts in the EU, since as explained above, it addresses some points which would hot be dealt with in case the only means available was the Convention. On the other hand, through the mandatory duty imposed upon the data processor, to report data breaches which are likely to result in a risk to the rights and freedoms of the data subject, to the national data protection authority, or to the data subject itself, in case of high risk, the GDPR increases transparency over data communications in a way the Convention is not.

One not so positive point (as it may lead to overlapping criminal sanctions) in this regard is that, in addition to the civil and administrative penalties foreseen in the GDPR, this legal document provides Member States with the possibility to lay down the rules on criminal penalties for infringements of the Regulation, including for infringements of national rules adopted pursuant to and within the limits of such Regulation[173].

The GDPR further mentions that "*the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice*".

The *ne bis in idem* principle is present both in Article 4 of Protocol no. 7 to the European Convention on Human Rights, and in Article 50 of the EU Charter of Fundamental Rights.

For such principle to apply, under both diplomas, there are four cumulative requirements, namely there must be two different criminal proceedings, which concern the same offence (the same typical illicit culpable and punishable act) and the same offender, under the same jurisdiction.

[173] Recital 149 of the GDPR.

However, the outlines of the principle have been refined by the CJEU jurisprudence.

In Case C-617/10[174], the Court ruled that the principle under analysis does not preclude a Member State from imposing successively, for the same acts, a tax penalty and a criminal penalty in so far as the first penalty is not criminal in nature, a matter which is for the national court to determine.

In this regard, the Court adds that it is up for the national court to establish whether a given penalty is criminal in nature, using the criteria established by the CJEU, namely: "*the legal classification of the offence under national law"; "the very nature of the offence*", which is to be assessed by reference to the aim of the provision, the persons to whom it is addressed and the legal right which it protects; and "*the nature and degree of severity of the penalty*"[175].

In Case C-537/16, the court ruled that, on what concerns the intrinsic nature of the offence, it is important to analyse whether the purpose of the penalty is punitive, because "*a penalty with a punitive purpose is criminal in nature for the purposes of Article 50 of the Charter*"[176].

Additionally, the Principle under analysis may be restricted under the conditions of Article 52 of the ECHR, according to which such limitations 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*".

In Case C-537/16, the CJEU ruled that "a *duplication of criminal proceedings and penalties may be justified*" in case they have complementary purposes[177].

---

[174] Case C-617/10 of the CJEU, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62010CJ0617&from=EN (last access on 29.10.2021), 2013, Paragraph 35, 37.

[175] Ibidem, paragraph 35.

[176] Case C-537/16 of the CJEU, available at: https://curia.europa.eu/juris/document/document.jsf?docid=200402&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=6133686 (last access on 29.10.2021), 2018, Paragraph 33.

[177] Summary of Case C-537/16 of the CJEU, available at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=9DAB3A62817A590A4B82603A

Additionally, in Case C-617/17[178], the CJEU ruled that the principle of *ne bis in idem* must be interpreted as not precluding a national authority from imposing a fine on an undertaking in a single decision for an infringement of national law and for an infringement of European law punishing the same conduct, as long as it ensures that the fines are proportionate to the nature of the infringement.

When employing such jurisprudence to the subject under analysis, it can be concluded that in jurisdictions where administrative fines do not have a punitive, the same offender can be convicted with both administrative fines and criminal penalties foreseen in the national legislation which executes the GDPR.

Moreover, even if the criminal penalties, established as a result of the permission to do so set forth in the GDPR, are not applied in a given case, the same offender is very likely to be prosecuted for the crime of illegal access or any other of the exposed above (depending on the means used to conduct the data breach), and simultaneously suffer the economic consequences of an administrative fine under national law, for disregarding the provisions of the GDPR.

Even though in accordance with the CJEU's jurisprudence these cases may not be regarded as infringing the *ne bis in idem* principle, the fact is that, in practical terms, the offender will suffer the consequences of his act twice, which is precisely what this principle means to prevent.

c. The Minimis Problem and the Enforcement Difficulties

Some Cybercrimes, when individually considered, tend to be of a small scale. Thus, victims often do not report them either because they do not notice their occurrence or because the impact those crimes have on their lives is not relevant enough for them to go through the burdens of reporting them to the competent

CB9E4F12?text=&docid=205205&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=711450 (last access on 29.10.2021), 2018, Paragraph 5.

[178]Case C-617/17 of the CJEU, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=212624&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1945668 (last access on 29.10.2021), 2019, Paragraph 39.

authorities[179], considering the level of bureaucracy involved and the lack of understanding on the process itself.

Additionally, some of these data related crimes are often reported directly to the bank, which assumes the loss and is therefore regarded as the real victim[180].

On the other hand, where victims are economic operators, reporting they suffered from a cyberattack may damage their image and reputation among customers and partners[181], exposing a weakness for competitors to explore[182], which is why more often than not, corporate targeted cybercrimes do not enter the statistics.

Moreover, as explained above, some jurisdictions, as is the case of Portugal, do not deem cybercrimes as public crimes, leaving it solely to the company to report it – if the company has no motivation in doing so, it is likely that the crime will go unpunished. Hence, also this lack of motivation to report may lead to the conclusion that criminal law is not the most suitable branch of law to achieve the effective prosecution of the perpetrator (at least not in its *status quo*).

Additionally, and still from a purely procedural law perspective, it must be noted that given all the aforementioned special elements of cybercrime, criminal law may not be the most suitable branch of law to address the conducts under analysis.

Firstly, it is likely that cybercrime diverges broadly, both in procedure and substance, from the daily police and judicial authorities' work. Thus, the gap in expertise between the perpetrator and police officers is so wide, it becomes really difficult to prosecute the perpetrator under the contours of criminal law.

---

[179] Bert-Jaap Koops, "The Internet and its Opportunities for Cybercrime", TRANSNATIONAL CRIMINOLOGY MANUAL, M. Herzog-Evans, ed., Vol. 1, pp. 735-754, Nijmegen: WLP, 2010; Tilburg Law School Research Paper No. 09/2011. Available at https://ssrn.com/abstract=1738223(last access on 29.10.2021), 2011, p. 745, 746.

[180] David Wall, "Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age". Corporate Hacking and Technology-Driven Crime: Social Dynamics And Implications, T. Holt, B. Schell, eds., pp. 68-85, Hershey, PA (USA): IGI Global, 2010. Available at: https://ssrn.com/abstract=1563626 (last access on 29.10.2021), 2010, p. 16.

[181] *Ibidem*, p. 16, 17.

[182] Mike Keyser, "The Council of Europe Convention on Cybercrime", 12 J. Transnat'l L. & Pol'y 287 (2002-2003), available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jtrnlwp12&div=14&id=&page= (last access on 29.10.2021), 2003, p. 289.

Ibidem, p. 16, 17.

Secondly, further difficulties arise when considering that the most often used technique to investigate a crime, is to study the crime scene, in order to identify the perpetrator and his *modus operandi*. However, most cybercrimes either do not have a crime scene, or in case they do, it is spread all over the web rather than being focused in a single physical location[183]. Analysing a cybercrime scene is as difficult as tracing all the data flows and different connections until the perpetrator's real IP is found. For that purpose, police officers may have to search through hundreds of computers located in different countries, where maybe cooperation mechanisms are not established, and some behaviours might not even be criminalized.

Another variable to consider is that the evidence of these crimes is digital evidence, which is not that hard to temper with and the means to get access to this intangible proof of crime, are extremely slow, even under existing judicial cooperation procedures. Not to mention the inefficiencies in cooperation between service providers and public authorities[184]. In this regard, and as referred above, the EU is preparing an e-evidence package which will simplify the process of acquiring digital evidence, shifting form a ten-step plan of formalities, to a four - step one[185] - recently, the European Parliament's Committee on Civil Liberties has actually voted in favour of a compromise proposal[186].

Additionally, it may be relevant to mention that the Council of Europe has already confirmed the author's understanding, stating that the lack of specialized expertise among prosecutors and judges is a major global concern, as judicial training on cybercrime and e-evidence is not as common as it should be[187], which means countries are underprepared for dealing with these data related crimes,

[183] Susan W. Brenner, "Cybercrime Metrics: Old Wine, New Bottles?", Virginia Journal Of Law & Technology Fall 2004 University Of Virginia Vol. 9, No. 13, available at: https://www.researchgate.net/publication/265032559_Cybercrime_Metrics_Old_Wine_New_Bottles/stats (last access on 29.10.2021), 2004, p. 8.
[184] Factsheet Security Union, "Facilitating access to electronic e-evidence", https://ec.europa.eu/info/files/factsheet-e-evidence_en (last access on 29.10.2021), 2018, p. 1.
[185] *Ibidem*, p. 3.
[186] European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, available at: https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html (last access on 29.10.2021), 2020.
[187] Council of Europe, "Capacity building on cybercrime Discussion paper", available at https://rm.coe.int/16802fa3e6 (last access on 29.10.2021), 2013, p. 17.

and even if law enforcement agents are able to track the perpetrator, the probability of him not being convicted is not that small.

For these reasons, insisting on addressing cybercrime through criminal law is, to a point, not only inappropriate but also contradictory, since the goal of prosecuting the offender is often unattainable.

On the other hand, on the substantive level, and assuming that even though the solution we have right now is not the most suitable, but is the existing one, departing from the principle that criminal law should be the last resort of a legal order, it is pertinent to ask whether some of these data related crimes actually pass the *de minimis* principle, according to which a certain behaviour should only be criminalised if it causes more than a minimum level of harm[188].

It is doubtful that, for instance, the right penalty for illegal access to someone's computer, with the sole purpose of self-recognition, is a criminal one[189].

However, if this practise is proceeded by hundreds of hackers in an organized manner, breaking into millions of computers at the same time, the impact might not be that minimal.

It is not easy to draw a line between which data related crimes should or should not be tackled by criminal law. Additionally, there are also some grey areas, such as data related cybercrimes that, despite being reprehensible and fitting into one of the typified crimes, have more positive than negative impact on society[190]. This is the case, for instance, when the victim of a cybercrime is a politician, and the data exposed relates to records of the illegal use of his governmental credit card, or the email records which illustrate the granting of illegal favours.

In the author's opinion, criminalizing online violations of data protection should not become a principle or tendency, which is precisely what is occurring now, being the crime of illegal access, the perfect example.

---

[188] *Ibidem*.

[189] Sofia Agostinho, "Online Violations of Data Protection – The Criminal Law Perspective", Essay submitted at Nova School of Law in the context of the Course "Cybersecurity", Spring Semester 2020, p. 9.

[190] The typical case is when a hacker illegally obtains evidence that proves the commission of certain impactful crimes and decides to expose it.

Nevertheless, it is also doubtful that drawing an abstract legal line dividing reprehensible from non-reprehensible behaviours is nearly impossible in this context. Hence, it is imperative to establish a case-by-case approach in order to access the presence of a given set of common abstract factors, in each specific case.

One possible approach, in this context, would be to add some more elements to the typified crimes, so that they take into account criteria which although typically used as aggravation circumstances, are also capable to warrant the crime implies a minimum level of harm – such criteria are the scale of impact caused to the victims, or the scale of the crime itself when considered as an organized crime. In the author's opinion, this dynamics would be capable to prevent scenarios where a given problem is tackled through criminal law, but civil law would also be effective, and sometimes even more suitable.

Directive 2013/40/UE, an EU legal instrument who also rules on the same matters as the international convention, adopts a similar approach in its Recital 11, where it provides for "*criminal penalties at least for cases which are not minor*". The Directive further clarifies what might be considered as a minor case, but ultimately leaves it to the Member States to decide. The criteria set forward in this legal instrument are, in turn, the damage caused by the offence, the risk to public or private interests, such as the integrity of computer data or system, the integrity or other interest of a given person[191].

The rationale behind this approach is based on the understanding that not all data related offenses have enough grounds to justify the offender going to prison, especially the minor ones.

Another possible solution would be to establish a principle based approach, where such principles could serve as guidelines for judges to decide, in each concrete case, whether a given conduct passes the minimal threshold referred herein.

[191] Namely, in its recital 11.

IV. CRIMINAL LIABILITY OF ELECTRONIC COMMUNICATIONS SERVICE PROVIDERS AND DIGITAL PLATFORMS FOR ONLINE VIOLATIONS OF DATA PROTECTION

Nowadays, a considerable number of the most successful companies all over the world operate online. Moreover, the most successful of them all tend to merely provide the channels necessary for third parties to conduct their own business.

Though this dynamics, the referred intermediary service providers, while not stating this publicly, advertise their services in a way which leads their addressable market to believe they do not ask for a counter performance in exchange for their services, when often they are collecting and processing their users' personal data for their own purposes, as a counter performance.

As we live in a world based on free will, such a scenario would not be so immoral, if it were not for the fact that such companies are proceeding without the data subject's complete awareness over how their personal data is being processed and the risks associated with providing such data without any discretion.

Without prejudice, it would also be immoral to argue that the platforms are to blame for exploiting the data user's general lack of information, inasmuch as they are nothing more than economic constructs with lucrative purposes, which are not meant to defend or educate their users, but rather to exploit their needs and provide services that correspond to them. The protectionist role is in fact up to the State and public economic powers, such as the United States or the European Union.

In the case of giant tech companies, it is important to keep in mind that the knowledge such companies possess over these topics is so wide that it deepens the gap between legislators and private sector even further, exacerbating the

aforementioned *pacing problem*[192]. Additionally, it is important to consider the economic means such companies have at their disposal to defend themselves.

Furthermore, the structure under which these companies operate often provides them with the possibility to resort to a liability exemption regime over the data transmitted through the platforms.

In this context, the focus lies on a triangular relationship between: the data subject, the trader (which is also a data subject and may also suffer from a cybercrime) and the provider of the online intermediary service (who obviously may also be the target of a cybercrime, even though even though the crimes committed against him are not the object of the analysis for the purposes of this chapter).

Whether we are talking about a trader or a consumer, for the purposes of this analysis either party of the contractual relationship shall be regarded as a user, as provided for in Article 2 (a) of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector[193].

Digital platforms are frequently regarded as intermediary service providers of information society services, as defined in Article 1 (1) of Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 and article 2 (a) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 [194].

As such, and as stated above, these service providers often benefit from a liability exemption taking away a great portion of their motivation to take preventive measures so that cybercrimes are not committed through their platforms.

[192] Gary Elvin Marchant, Braden R Allenby & Joseph R Herkert, "The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem", Springer Netherlands Available at: https://www.springer.com/gp/book/9789400713550 (last access on 29.10.2021), 2011.
[193] Namely, "*any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service*"
[194] Article 1 (1) of Directive 2015/1535; and article 2 (a) of Directive 2000/31/EC.

Such liability exemption first emerged so that digital platforms could be freely created and improve the online user experience[195]. Without a shred of doubt, it is the author's opinion that this approach is as appropriate to the needs felt by users and economic operators at the time the E-Commerce Directive entered into force, as it is inappropriate in the current context, where digital platforms have a monopoly over several business sectors.

Directive 2000/31/CE is the one where the liability of such stakeholders is foreseen. In this context, it is important to mention that even though Recital 54 provides Member States the option not to stipulate criminal sanctions for infringement of national provisions adopted pursuant to the Directive, it also indirectly states that such penalties may be stipulated, which is why it is pertinent to analyse such legal instrument here.

Additionally, the first Report on the application of the E-Commerce Directive also states that the liability limitations foreseen in the Directive under analysis are meant to cover both criminal and civil liability for illegal activities conducted by third parties[196].

With that in mind, this Directive foresees four different pillars, responsible for proving digital platforms with the possibility to grow all over the web. The first one is the establishment of the country-of-origin principle, which stipulates that such platforms would merely be subject to the laws of the country in which they were established[197]. The second pillar consists of the liability exemption regime, which will be further developed bellow. The third pillar represents the general prohibition for each Member State to impose an obligation for the platforms to monitor the information they transmit or store[198]. While the fourth pillar stands for the recommendation made in the Directive[199], for trade, professional and consumer

[195] Bart van der Sloot, "Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe", 6 (2015) JIPITEC, available at: https://www.jipitec.eu/issues/jipitec-6-3-2015/4318 (last access on 29.10.2021), 2015, p.212

[196] Commission of the European Communities, "First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0702&from=EN (last access on 29.10.2021), 2003, p.12.

[197] As provided for in Article 3 of the Directive.

[198] As provided for in Article 15 of the Directive.

[199] As provided for in Article 16 of the Directive.

associations or organizations to implement codes of conduct in order to contribute to the implementation of the Directive [200].

That said, there are three types of liability exemption foreseen in Directive 2000/31/CE. Firstly, Article 12 addresses the cases where the economic operators are merely access providers responsible for transmitting third-party information through their communication channels, or as named by the Directive in question, "*mere conduit*" service providers.

In this context, Article 12 stipulates that in cases where an information society service consists of the transmission in a communication network, the service provided shall not be liable for the information transmitted if he is not responsible for initiating the transmission, selecting its receiver and selecting or modifying the information contained in the transmission.

On the other hand, article 13 accounts for economic operators who may be regarded as caching providers, i.e., those that provide services consisting of automatic, intermediate and temporary storage of data in order to accelerate the information transmission[201].

For these purposes, Article 13 states that in cases where the recipient of the service provides a transmission in a communication network of information, the service provider shall not be liable for the automatic, intermediate and temporary storage of information aimed at increasing the efficiency of the information's transmission, as long as the five conditions foreseen by the law are met. Namely the provider shall not modify the information, he shall comply with the information's access conditions and updating rules, he shall not interfere with the technology in order to obtain data on the use of the information, and finally, he shall adopt the adequate measures to remove or disable access to the information in case he acknowledges such information has been removed or

[200] Miriam Buiten, Alexandre de Streel & Martin Peitz, "Rethinking Liability Rules for Online Hosting Platforms", Discussion Paper No. 074 Project B 05, available at: http://www.crid.be/pdf/public/8379.pdf (last access on 29.10.2021), 2019, p. 3.

[201] Anja Hoffmann & Alessandro Gasparotti, "Liability for illegal content online - Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a "Digital Services Act"", available at: https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepStudie_Haftung_fuer_illegale_Online-Inhalte/cepStudy_Liability_for_illegal_content_online.pdf (last access on 29.10.2021), 2020, p. 8.

blocked, or that one of the competent authorities have issued orders to remove or block such content.

Finally, if an act falls into the scope of Article 14, which accounts for economic operators who may be regarded as hosting providers, the requirements for the exclusion of this same liability are: the provider not having actual knowledge of illegal activity or information and, as regards claims for damages, he must not be aware of the facts or circumstances from which the illegal activity or information is apparent. In case such facts come to the service provider's attention, upon obtaining such knowledge or awareness, he shall the appropriate take action to remove or to disable access to the information.

Case L'Oréal v. eBay[202] provided some guidance in this regard, clarifying the circumstances which may indicate that an information society service provider has '*awareness'* within the meaning of Article 14(1) of the Directive.

Namely, the Court stipulates that this provision must be interpreted in the light, not only of its wording, but also of its context, and the goals pursued by the rules of which it is part[203]. It also adds that the present assessment must be carried in a case-by-case approach[204].

Furthermore, the CJEU asserts that in case the provider has conducted a merely technical and automatic processing of the data, Article 14(1) of Directive 2000/31/EC shall apply[205].

On the other hand, the liability exemption under analysis shall be waived, in case a diligent economic operator placed in the processor's circumstances, should have identified the illegality in question and operated in accordance[206].

Moreover, the CJEU states that Article 14(1)(b) must be interpreted as including every situation in which the provider concerned becomes aware of such facts or circumstances. "*The situations thus covered include, in particular, that in which*

[202] Case C-324/09 of the CJEU, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=107261&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6335951 (last access on 29.10.2021), 2011.
[203] *Ibidem*, Paragraph 111.
[204] *Ibidem*, Paragraph 65.
[205] *Ibidem*, Paragraph 113.
[206] *Ibidem*, Paragraph 120.

the operator of an online marketplace uncovers, as the result of an investigation undertaken on its own initiative, an illegal activity or illegal information, as well as a situation in which the operator is notified of the existence of such an activity or such information. In the second case, although such a notification admittedly cannot automatically preclude the exemption from liability provided for in Article 14 of Directive 2000/31, given that notifications of allegedly illegal activities or information may turn out to be insufficiently precise or inadequately substantiated, the fact remains that such notification represents, as a general rule, a factor of which the national court must take account when determining, in the light of the information so transmitted to the operator, whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality"[207].

Additionally, such liability exemptions shall only cover the cases where the "*activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient*" [208]. Basically, the economic operator must play a passive role – he must neither have knowledge nor control over the third party information which is transmitted or stored in its platform[209].

At this point, reference must be included as to the fact that, some jurisdictions foresee the possibility of legal persons being subject to criminal liability, namely, to cybercrime laws[210]. However, due to the liability exemption under analysis, at least on what comes to third-party information transmitted though the platform, of which they are not aware, such criminal liability is, *a priori*, excluded.

[207] *Ibidem*, Paragraphs 120, 121 and 122.
[208] Recital 42 of Directive 2000/31/CE.
[209] Sofia Lopes Agostinho, "A Responsabilidade das Plataformas Digitais pela Segurança dos Consumidores – A Propósito Do Ac. Do STJ, de 10/12/2020", Nova Consumer Blog, available at: https://novaconsumerlab.novalaw.unl.pt/a-responsabilidade-das-plataformas-digitais-pela-seguranca-dos-consumidores-a-proposito-de-ac-do-stj-de-10-12-2020/, 2021.
[210] Such as Portugal, for instance, where criminal liability of legal entities is specifically foreseen in Article 9 of the Cybercrime Law (Law No. 109/2009, from 15 September).

Thereby, the legislator deliberately opted to ensure the free movement of information society services between the Member States[211], to the detriment of the safety of users of such services.

It could be argued that it would be inappropriate to impose on such service providers the duty to monitor all activities carried out through their platforms. However, while this reasoning may be valid for small or medium-size intermediary service providers of information society services, as for the Internet giants, there will be no one in a better position than them to monitor the illicit activities pursued through their platforms.

Proof that even economic operators feel a responsibility to provide secure services and experiences is the recent YouTube case [212](as mentioned above), in which the operator illustrated the measures it has taken to protect its users, without necessarily being required to do so by law.

Additionally, other hosting platforms, such as Amazon, have their share of preventive measures. Amazon cooperates with other brands, to place unique barcodes in the products sold through their platform, so that it is possible to detect and remove counterfeit products from the platform. Furthermore, it uses a machine learning algorithm to help detect copyright violations[213].

Article 15 of the E-Commerce Directive further prohibits Member States from imposing a general obligation on service providers to monitor the information transmitted or stored, as well as from imposing an obligation to actively seek for facts or circumstances which indicate the commission of illegal activity.

Regardless of these conclusions, and specifically on what concerns intermediary service providers of information society services which fall under the scope of the legal definition of online marketplaces, the Commission's Communication on the

[211] As provided for in Article 1(1) of the Directive.
[212] In Joined Cases C-682/18 and C-683/18 of the CJEU, available at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=C50B2E6BBCC1BBCAD48EED6AEA3FE4DD?text=&docid=243241&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5935088 (last access on 29.10.2021), 2021, Paragraph 30.
[213] Miriam Buiten, Alexandre de Streel & Martin Peitz, "Rethinking Liability Rules for Online Hosting Platforms", Discussion Paper No. 074 Project B 05, available at: http://www.crid.be/pdf/public/8379.pdf (last access on 29.10.2021), 2019, p. 2.

Collaborative Economy[214] sets forward a group pf conditions that, when fulfilled, may indicate that the service provider shall be considered as actually providing the underlying service.

In this context, the criteria are: the platform setting the final price which will apply to the user; setting relevant terms and conditions (other than the price), which are determinant for the contractual relationship between the trader and the user; and in case the platform "*owns key assets used to provide the service*"[215].

The European Commission further suggests other relevant criteria. Namely, whether the service provider "*incurs the costs and assumes all the risks related to the provision of the underlying service*". Additionally, the existence of "*an employment relationship"* between the parties may also serve as a valid indicator[216].

Another aspect worthy to mention is that the Directive under analysis does not apply to questions related to information society services covered by the GDPR[217]. Hence, digital platforms shall be liable for unlawful processing of the user's personal data, namely if they collect and/or transmit personal data without a valid legal basis to do so. However, it is debatable whether such platforms should be able to invoke the liability exemption under analysis for the illegal processing of personal data conducted by their users, through the platform channels, as the Directive does not specify whether its non-applicability on GDPR related matters shall imply that the platform shall also be liable for unlawful processing of personal data by one of the platform's users, through the platform[218].

Article 29 Working Party further clarifies that "*An ISP providing hosting service is in principle a processor for the personal data published online by its customers, who use this ISP for their website hosting and maintenance. If, however, the ISP*

---

[214] European Commission, "A European agenda for the collaborative economy", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0356&from=EN (last access on 29.10.2021), 2016, p. 6.
[215] *Ibidem.*
[216] *Ibidem*.
[217] As provided for in Article 1 (5) (b) of the Directive.
[218] Mario Viola de Azevedo Cunha, Luisa Marin & Giovanni Sartor, "Peer-to-Peer Privacy Violations and ISP Liability: Data Protection in the User-Generated Web" (August 1, 2011). EUI Department of Law Working Papers No. 2011/011, Available at SSRN: https://ssrn.com/abstract=1953904 (last access on 29.10.2021), 2011, p. 58.

further processes for its own purposes the data contained on the websites then it is the data controller with regard to that specific processing"[219].

Nevertheless, this does not preclude the possibility of Member States imposing and monitoring obligations in a specific case. It also does not affect orders by national authorities in accordance with national legislation, nor the possibility for Member States to require service providers to apply "*duties of care*" which can reasonably be expected from them[220].

Overall, it is arguable that given the annual revenue some of these companies have, it is only fair that they are also deemed responsible for ensuring their users' safety within their networks and bear the costs (or at least a portion of it) associated with the browsing and contracts concluded through their platforms.

Examples of data related cybercrimes in this context are, for instance, the cases where someone buys a piece of software or even hardware which contains malicious code, programmed to cause harm to the consumer (which is, in this case, the affected data subject); or when a virus is spread via chat in the form of a link sent from an infected data user to all his network contacts.

Even though such service providers are not liable for the data transmitted through their channels, as explained above, there are some burdens on their side as well, namely, according to the Directive on privacy and electronic communications "*The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services*"[221]. For that purpose, a compromise must be made between implementation costs and the state of the art, without losing sight of the need for ensuring a security level appropriate to the risk presented. Additionally, in the case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers affected by that risk and, where the risk lies outside the scope of the

[219] Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of "controller" and "processor"", available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (last access on 29.10.2021), 2010, p. 25.
[220] Recital 47 and 48 of the Directive.
[221] Namely, in its Article 4.

measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

On the other hand, as regards unsolicited communications, the Directive states[222] that the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

However, this Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as the activities of the State in areas of criminal law, as provided for in Article 1 (3), hence, the penalty for non-compliance with such provisions shall not be a criminal, but rather civil or administrative one.

According to the CJEU case law, namely in the case C-673/17 (Case Planet 49)[223], such consent is not validly provided if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent.

Furthermore, the service provider must provide the user with relevant information, including the duration of the operation of cookies as well as whether or not third parties may have access to those cookies. Basically, consent should consist of an active rather than a passive user behaviour. Lack of a regular form of consent may imply the commission of a cybercrime by the platform, waiving the liability exemption, namely an illegal access cybercrime, as provided for in CoE Convention's Explanatory Report, in its recital no. 48.

A positive advance, in this context, is the one foreseen in the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act), which will amend Directive 2000/31/EC. Article 21 provides for the duty applicable to all online platforms, which do not

[222] Namely, in its Article 13.

[223] Case C-673/17 of the CJEU, "Case Planet 49", available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6141119 (last access on 29.10.2021), 2019, Paragraph 68 and 81.

qualify as a micro or small enterprise in the meaning of Recommendation 2003/361/EC, to inform law enforcement or judicial authorities of the Member State concerned, in case they become aware of any information giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place.

Even though Article 21 under analysis refers to criminal offenses which threat to the life or safety of a person, it must be referred that cybercrimes against privacy may actually fit such description. For instance, in case of illegal access to someone's location or illegal interference to a communication where the data subject is sharing confidential State information.

At this point, one might ask, considering digital platforms tend to have users from all around the world, which shall be the concerned Member State to contact in this case? For this purpose, it is further clarified in Article 21of the legal document under analysis, that the concerned Member State shall be the Member State where the offence is suspected to have taken place or is likely to take place, or alternatively, the Member State where the suspected offender or the victim resides or is located. Additionally, in cases where the platform cannot identify "*with reasonable certainty*"[224] the Member State concerned, it shall inform the law enforcement authorities of the Member State in which it is established or has his legal representative, or alternatively, it shall inform Europol.

Additionally, should a given user frequently provide manifestly illegal content, online Platforms shall suspend the provision of their services[225].

The legal representative, in this context, stands for the legal or natural person who acts as a representative in one of the European Union Member States, for the providers of intermediary services which do not have an establishment in the European Union but still offer their services there.

Another breakthrough provided for the Digital Services Act is the need for providers of intermediary services to publish a report on any content moderation

[224] Article 21 of the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act), which will amend Directive 2000/31/EC
[225] As provided for in Article 20 of the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act), which will amend Directive 2000/31/EC.

they engaged in. Additionally, the mechanisms which allow users to notify the providers of hosting services, of the presence on their services, of specific items that such user deems illegal[226], as well as internal complaint-handling systems[227], which most the tech giants already use, shall be deemed as mandatory, once the Digital Services Act comes into force.

Considering the overall picture of this recently issued legal document, progress has been made towards a safest online environment, especially since the duties it imposes on the platforms gradually evolve depending on their respective dimension. Nevertheless, one cannot ignore that the mere applicability of such liability exemption to very large online platforms[228] will amount to a lack of motivation on behalf of such companies, to further stipulate preventive measures, capable of exterminating a considerable portion of the existing online violations of data protection.

[226] As provided for in Article 14 of the diploma.
[227] As provided for in Article 17 of the diploma.
[228] I.e. online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million.

V. CONCLUSION

Cybercrime is an increasingly important branch of criminality, as data is more and more used as a counter performance for the provision of services (whether expressly indicated and admitted by the economic operators or not).

The data subject is not only subject to unlawful processing of his personal data, but also to an increasingly wide set of other cybercrimes against his personal data.

In an era where connectivity is perceived as a desirable next step for most of the already existing goods, and as a mandatory requirement for all the newly issued gadgets that enter the market, citizens are subject to data related cybercrimes not only when they are surfing the web on their smartphone or computer, but also on their smart TVs, smart watches, smart houses and so on.

In this context, it is about time that extraterritoriality and anonymity in cyberspace are appropriately tackled, for good.

For that purpose, each state will need to put their own sovereignty aside and decide to take on a collaborative approach on the topic of data related cybercrime in four mandatory fronts: first of all, there needs to be a minimum threshold of criminalization all around the globe, at least for data related cybercrimes, especially since a lot of national laws stipulate the principle of territoriality as a connection principle.

The existence of "*safe heavens*" is too easy for hackers to monetize for their own purposes. Hence, such legislative loopholes should not exist in order for cybercrime punishment to become possible/efficient.

Secondly, innovative methods need to be adopted by the legislator, so that the pacing problem be reduced, in order to avoid cases where a given subject is ruled by a mandatory legal system which becomes obsolete or inadequate to the society where it is applicable (like in the case of the E-Commerce Directive).

In this context, it is evident that erasing data related cybercrime diplomas and altering the offline corresponding type of crime in order to encompass this more complex and emerging form of crime, is not the correct approach. However, the legislator should definitely try to deem economic operators as allies on the task

of regulating cyberspace, and adopt one of the aforementioned innovative techniques to legislate, such as self-regulation diplomas approved by the competent state authorities or drafted under their supervision, or even the use of direct final rulemaking processes.

Furthermore, since most data protection related diplomas applicable to EU Member States are EU Regulations or Directives, it is about time for the EU legislator to compile all those documents in a data protection code, for the sake of consistency.

Thirdly, technical measures need to be taken, in order to assure that IP addresses cannot be ripped from any operating connected device. In this context, it is the author's opinion that the only way to ensure such a measure is adopted is to criminalize the manufacturing of devices where such rule is not addressed. This would obviously imply some effort from those who manufacture both software and hardware, but it would not be impossible. Considering next generations will rely more and more on personal data to provide services, it is about time to stop legislating in favour of the economic operator's freedom to operate, and start protecting each end every user.

Last but not least, it is also very important to spread a policy of transparency in the online world, for the prevention of data related cybercrimes, creating awareness among data users, on the dangers they face and which preventive measures must be taken. If people are not aware of the risks they face, they will never be able to protect themselves, regardless of how consistent and well designed, data protection laws are.

Another step for the EU legislator to consider is the creation of a legal regime applicable to data, which is not merely based on a liability rule, such as a non-transferrable property right which can be partially restricted through the stipulation of minor *in rem* rights. Additionally, the "*data-producer's right*" is a good complement to provide economic operators with some protection over their generated non-personal data.

As for the *minimis* threshold, criminalizing most online violations of data protection, should not be the first impulse when the desired result is the reduction of these intrusive behaviours. The first move should consist of an investment in

police and judicial capacity for the investigation and prosecution of such infractions, followed by a strong information strategy capable of providing Internet users with the proper knowledge and tools to face online dangers.

Additionally, all cybercrime laws should establish the necessary criteria, based on the impact and organized form of a given conduct, for criminal law to apply. However, considering the legislator decided to criminalize most data related offences, the minimum he should have done would be to make sure the enforceability of the typified data related offences was possible. Taking into account the special elements of cybercrime as well as the lack of the necessary tools not only by the Courts but also by the enforcement agencies, prosecuting cybercrime presents great challenges.

For that reason, putting some extra layer of liability on the side of the economic operator appears as a feasible solution, as such measure will certainly encourage them to take the appropriate measures to ensure cybercrimes are not committed through their platforms, especially if the alternative to non-compliance with the applicable rules were fines of a considerable amount of their annual revenue or income.

Additionally, the proper boundaries need to be created between the actions which are addressed by criminal law and those tackled by civil law. The CJEU must define concrete and unified contours explaining the limits imposed by the *ne bis in idem* principle, so that citizens can know what to expect from a given conduct.

BIBLIOGRAPHY

- Adam Smith, “The Wealth of Nations”, Oxford, England: Bibliomania.com Ltd, available at: https://www.loc.gov/item/2002564559/ (last access on 29.10.2021), 2002.
- Aleš Završnik, “Towards an Overregulated Cyberspace – Criminal Law Perspective.” Masaryk University journal of law and technology 4: 173-190, available at: https://journals.muni.cz/mujlt/article/view/2566 (last access on 29.10.2021), 2010.
- Allison Peters & Amy Jordan, “Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime”, available at: https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime (last access on 29.10.2021), 2019.
- Amalie W. Weber, “The Council of Europe's Convention on Cybercrime”, Berkeley Technology Law Journal Vol. 18, No. 1, Annual Review of Law and Technology (2003), pp. 425-446 (22 pages) Published By: University of California, Berkeley, School of Law, available at: https://www.jstor.org/stable/24120528 (last access on 29.10.2021), 2003.
- Andrii Shalaginov, Jan William Johnsen & Katrin Franke, “Cyber crime investigations in the era of big data", 2017 IEEE International Conference on Big Data, available at: https://www.researchgate.net/publication/322511369_Cyber_crime_investigations_in_the_era_of_big_data 2017 (last access on 29.10.2021), 2017.
- Anja Hoffmann & Alessandro Gasparotti, “Liability for illegal content online - Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a “Digital Services Act””, available at: https://www.cep.eu/fileadmin/user_upload/cep.eu/Studien/cepStudie_Haftung_fuer_illegale_Online-Inhalte/cepStudy_Liability_for_illegal_content_online.pdf (last access on 29.10.2021), 2020.

- Annika Suominen, “What Role for Legal Certainty in Criminal Law Within the Area of Freedom, Security and Justice in the EU?”, Bergen Journal of Criminal Law and Criminal Justice • Volume 2, Issue 1, 2014, pp. 1-31, Available at: https://www.legal-tools.org/doc/7d0cc5/pdf/ (last access on 29.10.2021), 2014.
- Article 29 Data Protection Working Party, “Guidelines on Personal data breach notification under Regulation 2016/679 (WP250rev.01)”, available at: https://ec.europa.eu/newsroom/article29/items/612052 (last access on 29.10.2021), 2017.
- Article 29 Data Protection Working Party, “Opinion 1/2010 on the concepts of "controller" and "processor"”, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (last access on 29.10.2021), 2010.
- Bart van der Sloot, “Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe”, 6 (2015) JIPITEC, available at: https://www.jipitec.eu/issues/jipitec-6-3-2015/4318 (last access on 29.10.2021), 2015.
- Bert-Jaap Koops & Ronald Leenes, Datenschutz und Datensicherheit 2006 (9), pp. 553-556., available at: https://www.researchgate.net/publication/228199147_ID_Theft_ID_Fraud_andor_ID-Related_Crime_-_Definitions_Matter (last access on 29.10.2021), 2006.
- Bert-Jaap Koops, “Criminal law and cyberspace as a challenge for legal research”, In: SCRIPTed, Vol. 9, No. 3, 2012, available at: http://script-ed.org/wp-content/uploads/2012/12/koops.pdf(last access on 29.10.2021), 2012.
- Bert-Jaap Koops, “The Internet and its Opportunities for Cybercrime”, TRANSNATIONAL CRIMINOLOGY MANUAL, M. Herzog-Evans, ed., Vol. 1, pp. 735-754, Nijmegen: WLP, 2010; Tilburg Law School Research Paper No. 09/2011. Available at https://ssrn.com/abstract=1738223(last access on 29.10.2021), 2011.

- Bradford W. Reyns, “Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses”, Journal of Research in Crime and Delinquency 50, no. 2 216–38, available at: https://doi.org/10.1177/0022427811425539 (last access on 29.10.2021), 2013.
- Case C-324/09 of the CJEU, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=107261&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6335951 (last access on 29.10.2021), 2011.
- Case C-537/16 of the CJEU, available at: https://curia.europa.eu/juris/document/document.jsf?docid=200402&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=6133686 (last access on 29.10.2021), 2018.
- Case C-617/10 of the CJEU, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62010CJ0617&from=EN (last access on 29.10.2021), 2013.
- Case C-617/17 of the CJEU, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=212624&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1945668 (last access on 29.10.2021), 2019.
- Case C-673/17 of the CJEU, “Case Planet 49”, available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6141119 (last access on 29.10.2021), 2019.
- Case United States of America, Appellee v. Microsoft Corporation, Appellant, 253 F.3d 34 (D.C. Cir. 2001), available at: https://law.justia.com/cases/federal/appellate-courts/F3/253/34/576095/ last access on 29.10.2021).
- Christopher L. Blakesley, "United States Jurisdiction over Extraterritorial Crime", The Journal of Criminal Law and Criminology (1973-) 73, no. 3 (1982): 1109-163, available at: https://doi.org/10.2307/1143188 (last access on 29.10.2021), 1973.

- Commission of the European Communities, “First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)”, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0702&from=EN (last access on 29.10.2021), 2003.
- Council of Europe “Convention on Cybercrime” “CoE Convention”, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 (last access on 29.10.2021), 2001.
- Council of Europe, “Capacity building on cybercrime Discussion paper”, available at https://rm.coe.int/16802fa3e6 (last access on 29.10.2021), 2013.
- Council of Europe, “Cybercrime Convention Committee T-YC Guidance Note #2, on Provisions of the Budapest Convention covering botnets”, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7094 (last access on 29.10.2021), 2013.
- Council of Europe, “European Convention on Mutual Assistance in Criminal Matters”, available at: https://rm.coe.int/16800656ce (last access on 29.10.2021), 1959.
- Council of Europe, “Explanatory Report to the Convention on Cybercrime”, available at: https://rm.coe.int/16800cce5b (last access on 29.10.2021), 2001.
- Council of Europe, “Recommendation N (99R) 5 of Council of Europe Committee of Ministers of the Committee of Ministers to Member States for the Protection of Privacy on the Internet”, available at: https://www.fd.unl.pt/docentes_docs/ma/MEG_MA_4009.pdf (last access on 29.10.2021), 1999.

- Council of Europe, “T-CY Guidance Note #7 – New forms of Malware - Adopted by the 9th Plenary of the T-C”, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e70b4 (last access on 29.10.2021), 2013.
- Council of Europe, “T-CY GUIDANCES NOTES Adopted by the 8th and 9th Plenaries of the T-C”, available at: https://rm.coe.int/16802e7132 (last access on 29.10.2021), 2013.
- Davey Winder, “This 20-Year-Old Virus Infected 50 Million Windows Computers In 10 Days: Why The ILOVEYOU Pandemic Matters In 2020”, Forbes Magazine, available at: https://www.forbes.com/sites/daveywinder/2020/05/04/this-20-year-old-virus-infected-50-million-windows-computers-in-10-days-why-the-iloveyou-pandemic-matters-in-2020/ (last access on 29.10.2021), 2019.
- David Wall, “Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age”. Corporate Hacking and Technology-Driven Crime: Social Dynamics And Implications, T. Holt, B. Schell, eds., pp. 68-85, Hershey, PA (USA): IGI Global, 2010. Available at: https://ssrn.com/abstract=1563626 (last access on 29.10.2021), 2010.
- Deloitte, “Cyber risk in an Internet of Things world Flashpoint edition 4: More data, more opportunity, more risk”, available at: https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html (last access on 29.10.2021).
- Directive 2019/770 of the European Parliament and of the Council of 20 May 2019, on certain aspects concerning contracts for the supply of digital content and digital services, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0770&from=EN (last access on 29.10.2021), 2019.
- Dirk Andreas Zetzsche, Ross P. Buckley, Douglas W. Arner & Janos Nathan Barberis, “Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation”, 23 Fordham Journal of Corporate and Financial Law 31-103 (2017), European Banking Institute Working Paper Series 2017 -

No. 11, University of Luxembourg Law Working Paper No. 006/2017, University of Hong Kong Faculty of Law Research Paper No. 2017/019, UNSW Law Research Paper No. 17-71, Center for Business and Corporate Law (CBC) Working Paper Series 001/2017, Available at: https://ssrn.com/abstract=3018534 (last access on 29.10.2021), 2017.

- EDPB, Guidelines 01/2021 on Examples regarding Data Breach Notification, available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en, 2021.
- Eric Rutger Leukfeldt & Majid Yar: "Applying Routine ActivityTheory to Cybercrime: A Theoretical and Empirical Analysis", available at http://dx.doi.org/10.1080/01639625.2015.1012409 (last access on 29.10.2021), 2016.
- European Commission, "A European agenda for the collaborative economy", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0356&from=EN (last access on 29.10.2021), 2016.
- European Commission, "Commission Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002&from=EN (last access on 29.10.2021), 2017.
- European Commission, "Communication on Building a European Data Economy", available at: https://digital-strategy.ec.europa.eu/en/library/communication-building-european-data-economy (last access on 29.10.2021), 2017.
- European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 2020", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en(last access on 29.10.2021), 2020.

- European Cybercrime Centre - EC3, “Combating crime in a digital age”, available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (last access on 29.10.2021).
- European Parliament & Council, “Directive (EU) 2016/1148 of the of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”, available at: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32016L1148 (last access on 29.10.2021), 2016.
- European Parliament & Council, “Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)”, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN (last access on 29.10.2021), 2017.
- European Parliament & Council, “Regulation (EU) 2016/679 of the 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)”, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN(last access on 29.10.2021), 2016.
- European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, available at: https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html (last access on 29.10.2021), 2020.
- European Union, “Charter of Fundamental Rights (2012/C 326/02)”.
- EUROPOL, “Botnet Taken Down Through International Law Enforcement Cooperation”, available at: https://www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation (last access on 29.10.2021), 2015.

- EUROPOL, "EC3 Partners", available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners (last access on 29.10.2021).
- EUROPOL, "International Action Against 'Gameover Zeus' Botnet And 'Cryptolocker' Ransomware", available at: https://www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware (last access on 29.10.2021), 2014.
- Europol, "Internet Organised Crime Threat Assessment" (Iocta), available at: https://perma.cc/N8HQ-CZT9 (last access on 29.10.2021), 2018.
- EUROPOL, "Users of Remote Access Trojans Arrested in EU Cybercrime Operation", available at: https://www.europol.europa.eu/newsroom/news/users-of-remote-access-trojans-arrested-in-eu-cybercrime-operation (last access on 29.10.2021), 2014.
- Factsheet Security Union, "Facilitating access to electronic e-evidence", https://ec.europa.eu/info/files/factsheet-e-evidence_en (last access on 29.10.2021), 2018.
- FGCE, "Strengthening cyber capacity and expertise globally through international collaboration", available at: https://thegfce.org/ (last access on 29.10.2021).
- Gary Elvin Marchant, Braden R Allenby & Joseph R Herkert, "The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem", Springer Netherlands Available at: https://www.springer.com/gp/book/9789400713550 (last access on 29.10.2021), 2011.
- Herbert Zech, "Information as Property", 6 (2015) JIPITEC 192, available at: https://www.jipitec.eu/issues/jipitec-6-3-2015/4315/zech%206%20(3).pdf (last access on 29.10.2021), 2015.
- Howard F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues", Software Engineering Institute, available at:

https://resources.sei.cmu.edu/asset_files/SpecialReport/2002_003_001_13928.pdf (last access on 29.10.2021), 2002.

- Investopedia, "Big Data", available at: https://www.investopedia.com/terms/b/big-data.asp (last access on 29.10.2021), 2021.
- Investopedia, "Data Analytics", available at: https://www.investopedia.com/terms/d/data-analytics.asp (last access on 29.10.2021), 2021.
- Investopedia, "Data Mining" available at: https://www.investopedia.com/terms/d/datamining.asp (last access on 29.10.2021), 2021.
- Ionita Gheorghe Iulian, "Trends and Developments in Use and Implementation of Cybercrime Convention", 2015 Conf. Int'l Dr. 870, available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/cidstue2015&div=116&id=&page= (last access on 29.10.2021), 2015.
- Ivan Stepanov, "Introducing a property right over data in the EU: the data producer's right – an evaluation", International Review of Law, Computers & Technology, 34:1, 65-86, available at: https://www.tandfonline.com/doi/pdf/10.1080/13600869.2019.1631621?needAccess=true (last access on 29.10.2021), 2020.
- Jeff Kosseff, "8. A Lawless No-Man's Land?" In The Twenty-Six Words That Created the Internet, 167-189. Ithaca, NY: Cornell University Press, available at: https://doi.org/10.7591/9781501735783-010 (last access on 29.10.2021), 2019.
- Jeff Petters, "What is a Proxy Server and How Does it Work?", available at: https://www.varonis.com/blog/what-is-a-proxy-server/ (last access on 29.10.2021), 2021.
- John Perry Barlow, "A Declaration of the Independence of Cyberspace", John Perry Barlow Library, available at: https://www.eff.org/cyberspace-independence (last access on 29.10.2021), 1996.
- Joined Cases C-682/18 and C-683/18 of the CJEU, available at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=C50B2E6

BBCC1BBCAD48EED6AEA3FE4DD?text=&docid=243241&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5935088 (last access on 29.10.2021), 2021.

- Jonathan Clough, "Principles of Cybercrime, available at: https://www.cambridge.org/core/books/principles-of-cybercrime/F172001ECA8742B5C3E0678CDF977718 (last access on 29.10.2021), 2015.
- Jonathan Clough, "Principles of Cybercrime, available at: https://www.cambridge.org/core/books/principles-of-cybercrime/F172001ECA8742B5C3E0678CDF977718 (last access on 29.10.2021), 2015.
- Jorge de Figueiredo Dias, "Direito Penal Parte Geral Tomo I – Questões Fundamentais a Doutrina Geral do Crime", Gestlegal 3rd Edition, available at: https://www.almedina.net/direito-penal-parte-geral-tomo-i-1574259663.html (last access on 29.10.2021), 2017.
- Kamal Ahmad & UNITAR, "The law of cyber-space : an invitation to the table of negotiations", United Nations Digital Library, available at: https://digitallibrary.un.org/record/566838 (last access on 29.10.2021), 2005.
- Laurence Lessig, "Code and Other Laws of Cyberspace", New York, Basic Books, available at: https://dl.acm.org/doi/10.5555/555000 (last access on 29.10.2021), 1999.
- Lawrence E. Cohen & Marcus Felsen, "Social Change and Crime Rate Trends: a Routine Activity Approach", American Sociological Review 1979, Vol. 44 (August), available at: http://www.personal.psu.edu/users/e/x/exs44/597b-Comm%26Crime/Cohen_FelsonRoutine-Activities.pdf (last access on 29.10.2021), 1979.
- Majid Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory", European Journal of Criminology 2, no. 4 (October 2005): 407–27, available at: https://doi.org/10.1177/147737080556056 (last access on 29.10.2021), 2005.

- Mario Viola de Azevedo Cunha, Luisa Marin & Giovanni Sartor, “Peer-to-Peer Privacy Violations and ISP Liability: Data Protection in the User-Generated Web” (August 1, 2011). EUI Department of Law Working Papers No. 2011/011, Available at SSRN: https://ssrn.com/abstract=1953904 (last access on 29.10.2021), 2011.
- Mark Fenwick, Wulf A. Kaal & Erik P.M Vermeulen, “Regulation Tomorrow: What Happens When Technology Is Faster Than the Law?”, American University Business Law Review, Vol. 6, No. 3, 561; U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-20, Available at SSRN: https://ssrn.com/abstract=3204119 (last access on 29.10.2021), 2017.
- Mike Keyser, “The Council of Europe Convention on Cybercrime”, 12 J. Transnat'l L. & Pol'y 287 (2002-2003), available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jtrnlwp12&div=14&id=&page= (last access on 29.10.2021), 2003.
- Ming-Li Hsieh & Shun-Yung Kevin Wang, “Routine Activities in a Virtual Space: A Taiwanese Case of an ATM Hacking Spree”. International Journal of Cyber Criminology, 12(1), 333–352, available at: https://doi.org/10.5281/zenodo.1467935Hsieh (last access on 29.10.2021), 2018.
- Miriam Buiten, Alexandre de Streel & Martin Peitz, “Rethinking Liability Rules for Online Hosting Platforms”, Discussion Paper No. 074 Project B 05, available at: http://www.crid.be/pdf/public/8379.pdf (last access on 29.10.2021), 2019.
- Mohan Krishna Kagita, Navod Thilakarathne, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, & Saurabh Singh, “A Review on Cyber Crimes on the Internet of Things”, in: ResearchGate, available at: https://www.researchgate.net/publication/344244881_A_Review_on_Cyber_Crimes_on_the_Internet_of_Things (last access on 29.10.2021), 2020.
- Nadezda Purtova, “Property in Personal Data: a European Perspective on the Instrumentalist Theory of Propertisation”, European Journal of Legal Studies, 2010, 2, 3, The Future of Law & Technology in the Information Society, available at: https://core.ac.uk/download/pdf/45678038.pdf (last access on 29.10.2021), 2010.

- OECD, “Computer Viruses and Other Malicious Software: A Threat to the Internet Economy”, OECD Publishing, Paris, available at: https://doi.org/10.1787/9789264056510-en, (last access on 29.10.2021), 2009.
- “Paris Call for Trust and Stability in Cyberspace”, available at: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf (last access on 29.10.2021), 2018.
- Parlamento, “Competências da Assembleia da República”, available at: https://www.parlamento.pt/Parlamento (last access on 29.10.2021).
- Pº C.P. 11/2004 DSJ-CT., “Usufruto simultâneo e sucessivo”, available at: https://www.irn.mj.pt/IRN/sections/irn/doutrina/pareceres/predial/2004/p-c-p-11-2004-dsj-ct/downloadFile/file/pcp011-2004.pdf?nocache=1315923809.68 (last access on 29.10.2021).
- Press release: “E-evidence package: Council agrees its position on rules to appoint legal representatives for the gathering of evidence”, available at: https://www.consilium.europa.eu/en/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence (last access on 29.10.2021), 2019.
- Ralph Gross & Alessandro Acquisti, "Information Revelation and Privacy in Online Social Networks (The Facebook case)." Paper presented at the meeting of the ACM Workshop on Privacy in the Electronic Society (WPES), Alexandria, available at: https://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf (last access on 29.10.2021), 2005.
- Rob Sobers, “98 Must-Know Data Breach Statistics for 2021”, Varonis, 4. 16, 2021, available at https://www.varonis.com/blog/data-breach-statistics/ (last accessed on 29.10.2021), 2021.
- Ronald M. Levin, “Direct Final Rulemaking”, George Washington Law 64: 1–34, available at: https://www.acus.gov/sites/default/files/documents/1995-04%20Pt.2%20Procedures%20for%20Noncontroversial%20and%20Expedited%20Rulemaking.pdf (last access on 29.10.2021), 1995.

- Russell Ackoff., “From Data to Wisdom.” In Ackoff’s Best, 170–172. New York: John Wiely and Sons, available at: https://faculty.ung.edu/kmelton/Documents/DataWisdom.pdf (last access on 29.10.2021), 1999.
- Ryan Hagemann, Jennifer Huddleston & Adam D. Thierer, “Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future”, Colorado Technology Law Journal, Available at SSRN: https://ssrn.com/abstract=3118539 (last access on 29.10.2021), 2018.
- Sofia Agostinho, “Online Violations of Data Protection – The Criminal Law Perspective”, Essay submitted at Nova School of Law in the context of the Course “Cybersecurity”, Spring Semester 2020.
- Sofia Lopes Agostinho, “A Responsabilidade das Plataformas Digitais pela Segurança dos Consumidores – A Propósito Do Ac. Do STJ, de 10/12/2020”, Nova Consumer Blog, available at: https://novaconsumerlab.novalaw.unl.pt/a-responsabilidade-das-plataformas-digitais-pela-seguranca-dos-consumidores-a-proposito-de-ac-do-stj-de-10-12-2020/, 2021.
- Sofia Ranchordas, “Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation” (November 1, 2014). Jurimetrics, Vol. 55, No. 2, Available at SSRN: https://ssrn.com/abstract=2544291 (last access on 29.10.2021), 2015.
- Special Eurobarometer 499, Europeans’ attitudes towards cyber security, available at: https://op.europa.eu/pt/publication-detail/-/publication/468848fa-49bb-11ea-8aa5-01aa75ed71a1 (last access on 29.10.2021), 2020.
- Summary of Case C-537/16 of the CJEU, available at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=9DAB3A62817A590A4B82603ACB9E4F12?text=&docid=205205&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=711450 (last access on 29.10.2021), 2018.
- Susan W. Brenner, “Cybercrime Metrics: Old Wine, New Bottles?”, Virginia Journal Of Law & Technology Fall 2004 University Of Virginia Vol. 9, No. 13, available at:

https://www.researchgate.net/publication/265032559_Cybercrime_Metrics_Old_Wine_New_Bottles/stats (last access on 29.10.2021), 2004.

- Tor Project, “Browse Privately. Explore Freely.”, https://www.torproject.org/ (last access on 29.10.2021).
- Tseloni, Andromachi, Karin Wittebrood, Graham Farrell, & Ken Pease, "Burglary Victimization in England and Wales, the United States and the Netherlands: A Cross-National Comparative Test of Routine Activities and Lifestyle Theories." The British Journal of Criminology 44, no. 1 (2004): 66-91, available at: http://www.jstor.org/stable/23639022 (last access on 29.10.2021).
- UNCTAD, “Cybercrime Legislation Worldwide”, available at: https://unctad.org/page/cybercrime-legislation-worldwid (last access on 29.10.2021), 2020.
- UNDOC, “Obstacles to cybercrime investigations”, available at: https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html (last access on 29.10.2021), 2019.
- United Nations Economic and Social Council (2018-2019 : New York and Geneva), “Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing : resolution / adopted by the Economic and Social Council”, available at: https://digitallibrary.un.org/record/3814466#record-files-collapse-header (last access on 29.10.2021), 2019.
- United Nations, “Convention Against Transnational Organized Crime and the Protocols Thereto”, available at: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf (last access on 29.10.2021), 2004.
- United Nations, “Treaty Collection”, available at: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en (last access on 29.10.2021), 2021.
- UNODC United Nations Office on Drugs and Crime, “Comprehensive Study on Cybercrime”, available at: http://www.unodc.org/documents/organized-

crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (last access on 29.10.2021), 2013.

- Uta Kohl, “Eggs, Jurisdiction, and the Internet”, International and Comparative Law Quarterly 51, no. 3 (2002), available at: https://doi.org/10.1093/iclq/51.3.555 (last access on 29.10.2021), 2008
- World Economic Forum, “Centre for Cybersecurity”, available at: https://www.weforum.org/centre-for-cybersecurity/ (last access on 29.10.2021).