„BABEȘ-BOLYAI” UNIVERSITY

FACULTY OF LAW

CYBER DEFENCE PROTECTION OF PRIVATE LIFE PERFORMED BY INTERMEDIARIES

(SUMMARY AND OVERVIEW)

Scientific coordinator:

Prof. Univ. Dr. Vasiu Ioana

PhD candidate:

Gabudeanu Larisa

Cluj-Napoca

2024

In the last decades, the number of online services to customers has grown as well as the number of customers that choose to obtain online services. For consumers, a significant number of transactions concerning products and services are conducted online, through various intermediaries. According to a study conducted by Capgemini, around 1.3 trillion non-cash transactions were performed globally in 2023 from around 500 billion in 2018.[1] Further, in terms of marketing towards consumers, the profiling of consumers in view of identifying their preferences is widespread and usually used across multiple platforms.[2] Consequently, individuals are increasingly using internet resources for

Also, in terms of relations between authorities and citizens, various IT projects have been created for the main interaction among the two, including payment of taxes, issuance of official documents, public procurement procedures, tax/fiscal information, litigation proceedings, electronic access to case files in litigation and criminal prosecution, nationwide examinations in schools and elections in electronic form. The best example in this respect is Estonia, with its e-

[1] Capgemeni, Global non-cash transaction vulumes, 2023, https://www.capgemini.com/news/press-releases/global-non-cash-transaction-volumes-set-to-reach-1-3-trillion-in-2023/ , last accessed on 16 October 2023. Capgemini and BNPP, 2018 World Payments Report, https://www.worldpaymentsreport.com, last accessed on 28 December 2022.
[2] Parker, Clifton, New Stanford research finds computers are better judges of personality than friends and family, 2015, https://news.stanford.edu/2015/01/12/personality-computer-knows-011215/, last accessed on 24 December 2022.

government approach.[3] This has also been generating a large amount of data pertaining to individuals to be stored and processed by public authorities.

For this purpose, the focus of this thesis is the role of intermediaries (defined as operating systems, browsers, application stored and hardware) in ensuring prevention measures are in place to protect individuals. We have chosen this viewpoint as the intermediaries are best placed to enhance the existing preventive measure legal requirements given their unique access to data and possibility of interaction with the individuals. In terms of the objectives of this thesis, we first focus on identifying the intrusiveness in the context of ensuring security to individuals. To this end, we included an analysis limitations to automated decision-making for security purposes, use of active defence mechanisms, as well as data protection and criminal law limitations to data collection, data aggregation and data sharing with authorities and private entities. This is correlated throughout the thesis with the technical constrains of intermediaries in terms of identification of cyber threats or of cyber-attacks or in terms of preventing these. This is highly relevant in terms of setting-up proper roles and responsibilities within the digital ecosystem that reflect the technical real-life scenarios. An outline of the objectives is included below:

Objective 1: Establish criteria for identifying intrusiveness in the context of ensuring security to individuals. This takes into account data collected, data aggregated (profiling), data disclosed and notifications, together with amendments to be brought to criminal law and data protection legislation.

Sub-objective 1.1: Identifying limits to security measures through implementation of data minimisation (including in aggregation of data and sharing of data) and automated decision-making data protection requirements.

Sub-objective 1.2: Possibility of using certain types of active defence under existing legislation and proposal of changes to data protection and criminal law legislation to accommodate these and sharing of data with other intermediaries or other entities.

Objective 2: Identifying role to be defined for intermediaries (operating systems, hardware providers, browsers, application stores) in terms of ensuring security, while also balancing privacy (including lack of intrusiveness).

Sub-objective 2.1: Changes that are needed to existing legislation in order to ensure accountability of these intermediaries, as their role and obligations are not fully covered by existing legislation by reference to real-life involvement of these intermediaries in the data processing of individuals.

Sub-objective 2.2: Proposed changes to existing data protection and criminal law legislation in view of ensuring possibility of security measures ensured by the intermediaries and, at the same time, limits to the types of security measures that can be taken, given the legal and technical limitations in this respect.

The result of the analysis includes gaps identified in current criminal law and related legislation, together with legislative proposals for setting in place relevant legal requirements for

[3] INSEAD/WIPO, 2017 report - Global Innovation Index 2017 Report, https://www.globalinnovationindex.org/gii-2017-report, last accessed on 28 December 2022. WIPO, Global Innovation Index, 2023, https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2023-en-main-report-global-innovation-index-2023-16th-edition.pdf, last accessed on 21 October 2023.

the role of intermediaries in the prevention of breaches to private life of individuals. The main results which constitute a novelty brought by this thesis include the following aspects:

- Proposal for enhancement of private life concept in view of reflecting the digital data stored and used by individuals and the risk associated therewith.
- New obligations for intermediaries in terms of prevention of cyber-threats and cyber-attacks, by reference to the data to which they have access to, the possibility to interact with the individuals/users (and with authorities and other private entities), but also by reference to the technical and operational limitations in identifying or addressing cyber-threats and cyber-attacks.
- Regulating risk-based approach to obligations of intermediaries and, thus, correlated risk-based approach analysis to have in mind when establishing criminal liability.
- User involvement and liability in certain limited use cases in which his/her input or action are needed and in case of inaction/action with intention.
- Possibility of intermediaries to establish active defence mechanisms and level of actions that can be taken considering criminal law implications of such actions.
- Possibility to extend self-defence measure for actions performed by intermediaries on behalf of the user.
- Legal limitations concerning aggregation of data from multiple users and requirements for anonymisation thereof.
- Mechanism of cooperation between intermediaries and authorities or other digital stakeholders, while observing existing criminal law and data protection limitations.

In terms of research methodology, firstly, we made an analysis and comparison of main characteristics of intrusiveness in criminal law and data protection case law and data protection sanctions in the EU (legislation, case law and implementation guidelines in the criminal law, human rights and data protection domains). Secondly, we performed an analysis of the balance between security and privacy in legal doctrine, case law and data protection sanctions at the EU and Romanian law levels in terms of the legislation currently in force and draft proposals, together with US best practices outlined in legal doctrine and relevant for the EU legal system.

Through these two methods we identified the role of intermediaries in the current EU legislation and any limitations in terms of implementing an obligation for intermediaries to ensure proper preventive security measures. In view of practical applicability of the objectives and hypothesis, we made a comparison between multiple privacy and security policies/features of intermediaries – at least 3 from each category – operating system, browser, and application store provider on a particular set of criteria to identify the manner in which they currently address preventive measures for security of the private life of their users. In addition, for the results of the above analysis, we included a validation of identified gaps in legislation, limitations of legal and technical nature in ensuring proper security of the private life of individuals through quantitative questionnaire on individuals (end-users), legal advisors and IT experts. The outcome and conclusions from the questionnaire are included at the end of each section within the thesis.

The concept o private life has emerged in terms o European legislation from the human rights conventions to the data protection legislation and to the criminal law conventions. Nevertheless, this concept and its protection has been envisaged more in terms o physical landscape and limited in terms of digital landscape, as shown in this chapter and in title II below. We have identified certain limitations in the definition of the criminal offence of breach of private

life in EU level legislation and Romanian law[4] level by reference to the changing digital world in which the private life is more and more digitalised with respect to certain intermediaries: operating system, browser, application store and hardware provider. As detailed below, there is a lack of proper legal requirements for security measure to prevent breach of private life, with such legal requirements being applicable for a category of stakeholders in the digital ecosystem, respectively, the intermediaries mentioned above. [5]

The types of data analysed in this thesis include data stored on the user device and on the server of the online service used by the user (including servers of sub-contractors of the online service provider).[6] The data includes structured and unstructured types of data which refers to content created, uploaded or received by the user and interaction of the user with the device, the online service or the environment and the data concerning the (potential) perpetrators or in relation to IT systems used by the perpetrators.[7] The thesis brings additional insights into expanding the definition of private life to accommodate current use of digital devices and data in an interconnected world.

The thesis also emphasises the need for further clarity in case intermediaries are used for such activities. This entails also the cooperation mechanisms in place and needed to be set in place in view of cooperating with other private entities and authorities (either criminal investigation authorities of cyber security authorities). Working Party Article 29[8] has also emphasised the need to address the role of online intermediaries by reference to the technical and economical role of each type of such intermediaries. Intermediaries such as operating systems, browsers and hardware providers are the ones that interact most with the individuals online and they have the widest overview of the individual's activity online.[9]

Given the legislative background mentioned above, there are two angles that require further research and clarification. One related to the usefulness of user profiling and monitoring in order to ensure proper security measures[10] and the other to the need to share data between various stakeholders in the same industry or across industries in order to ensure implementation of proper preventive security measures before occurrence of security incidents.[11]

Further, in terms of preventive steps for protection of private life, in the context of digital landscape there are limited legal requirements in this respect, as detailed below. This thesis identifies the lack of legal provisions that clearly establish the level of security measures that

---

[4] Slavoiu, Radu, Protectia penala a vietii private, Universul Juridic, pag. 152, 2016

[5] Gasser, U. and Schulz, W. Governance of Online Intermediaries: Observations From a Series of National Case Studies. Harvard University Berkman Center for Internet and Society Research Publication Series, No. 2015-5. Boston. http://dx.doi.org/10.2139/ssrn.2566364, last accessed on 8 December 2022.

[6] Acharya, S.; Rawat, U.; Bhatnagar, R. A Comprehensive Review of Android Security: Threats, Vulnerabilities, Malware Detection, and Analysis. Secur. Commun. Netw. 2022.

[7] Maimon, David, Louderback, Eric R., Cyber-dependent crimes: An interdisciplinary review, Annual Review of Criminology 2, pp. 191-216, 2019.

[8] Working Party Article 29, Working Document, Privacy on the Internet – An Integrated EU Approach to On-line Data Protection, 2000.

[9] Timis Tribunal, decision no. 166/2017 concerning potential liability of a data center owner for illegal activities performed using the servers in the data center.

[10] Schiopu, Silviu-Dorin, Privire generală asupra măsurilor tehnice şi organizatorice necesare pentru implementarea efectivă a Regulamentului general privind protecţia datelor, Revista Romana de Drept al Afacerilor 2/2019, 2019.

[11] NIS Cooperation Group, Reference document on security measures for Operators of Essential Services, CG Publication 01/2018, 2018.

should be implemented by private entities in order to ensure protection of privacy rights.[12] This also includes the involvement of third parties in the determination of and in the setting-up of preventive security measures. In addition, the thesis outlines proposed improvements to clarifying the role of each stakeholder and the limitations of the security measures obligations.[13]

Given the above new angles of analysis of existing legal requirements, this thesis opens up the discussions with respect to a couple of points where there is an intersection between data protection and criminal law legal provisions.[14] In addition, the research brings to light the issues that arise from the technical aspects of cyber-threats and cyber security prevention mechanisms, together with their limitations. There is a very thin line between the actions a company can take to protect their data and the infringing on rights of rights of other individuals (e.g. perpetrators, holder of IT systems used during the perpetration of a criminal offence).[15]

The aim of this thesis is to analyse this thin line and determine the situations which constitute a legitimate manner of ensuring security measures, together with proposals of changes in legislation or in interpretation (depending on the economic and technical opportunity of such changes). Given the general wording of security measure implementation legislation, the implementation thereof in practice has evolved mainly based on private sector practice and standards. Further, there is an interplay between legal requirements in terms of security (e.g. NIS Directive, banking legislation, GDPR) [16] and in terms of privacy protection (e.g. ECHR, GDPR, Budapest Cybercrime Convention, Romanian Criminal Code).

This thesis brings a new light on the obligation to ensure preventive security technical and organisational measures, as it analysis the limitations of usually researched active defence and of data sharing based on data protection and criminal law obligations.[17] Even if not expressly regulated as a security measure, the gathering of information about existing cyber-attack patterns and perpetrators is useful information in order to structure a resilient IT system in a private entity.[18]

Title II refers to framing the context of private life and intrusiveness role from the criminal, data protection and human rights perspective in view of enhancing the current context of the criminal legislation.[19] Chapter II.1 analyses the concept of private life and intrusiveness under different types of legislation. To this end, in chapter II.2 there is also an analysis on the intrusiveness implications on private life in the context of profiling and automated decision making, which is one of the most essential aspects given the digital ecosystem and its reliance on

---

[12] ENISA, Proactive Detection of Security Incidents, 2012. Ioana, Martin, Detectarea proactive a atacurilor cibernetice – honeypot-urile, Revista de investigare a criminalitatii, suppl. Special Issue 1; Bucharest vol. 8, Iss. 1, pp. 151-157, 2015.

[13] Moore R., The Case for Regulating Quality within Computer Security Applications, in European Journal of Law and Technology, vol. 4, No. 3, 2013. Kristin E. Heckman et al., Cyber Denial, Deception and Counter Deception A Framework for Supporting Active Cyber Defense, 2015. Arthur Cockfield, Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance, 29 Queen's Law Journal, pp. 364-407, 2003.

[14] Walters, Robert, Novak, Marko, Cyber Security, Artificial Intelligence, Data Protection and the Law, Springer, 2021.

[15] Maimon, David, and Eric R. Louderback, Cyber-dependent crimes: An interdisciplinary review, Annual Review of Criminology 2, pp. 191-216, 2019.

[16] Schünemann, W., Baumann, M-O, Privacy, Data Protection and Cybersecurity in Europe, Springer, 2017.

[17] Hathaway, Oona et al., The Law of Cyber-Attack, California Law Review 100(4), 2011.

[18] Cheng, B.; Kikuta, T.; Toshimitsu, Y.; Saito, T. Investigation of Power Consumption Attack on Android Devices. In Proceedings of the International Conference on Advanced Information Networking and Applications, Toronto, ON, Canada, 12–14 May 2021; Springer: Berlin/Heidelberg, Germany, pp. 567–579, 2021.

[19] Ho, Heemeng, Ko, Ryan, Mazerolle, Lorraine, Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review, Computers and Security, vol. 115, 2022, https://doi.org/10.1016/j.cose.2022.102611.

processing large amounts of data and providing real-time responses.[20] In addition, chapter II.3 reviews the manner in which certain technical capabilities in terms of use of honeypots and active defence mechanisms can be used to ensure proper prevention of cyber-attacks, recovery of stollen data (or deletion thereof) and apprehension of the perpetrator.

Chapter II.1 focuses on sub-objective 1.1 and hypothesis 1.1.1 in view of identifying the concept of intrusiveness and how this relates to private life in view of proposing an enhancement of the existing private life concept under the criminal offence of private life in the Romanian Criminal Code.[21] To this end, the chapter starts with Section II.1.1 focusing on the concepts of intrusiveness and private life, continues with the data covered by the concept of private life in Section II.1.2 and includes related privacy harms to be had in mind for the analysis of breach of private life in Section II.1.4, whereas Section II.1.5 focuses on the location of such data or of the user in view of determining the impact thereof on the protection of private life.[22] The role of consent is especially important in this context as it is one of the main manners in which certain breach of private life occur and this is analysed in Section II.1.4. [23]

Chapter II.2 refers to sub-objective 1.1 that refers to hypothesis 1.1.2, as the prevention mechanisms, to be effective entail automation and aggregation of data. Such aspects have certain legal limitations in the current legislation. [24] However, there are certain points that are still not fully addressed and that require additional legal provisions. The chapter also addresses hypothesis 1.1.3, which is related to anonymisation/pseudonymization and the need for further legal regulation in this respect in terms of the use of anonymisation/pseudonymization techniques for automated decision making in the context of security measures.[25]

Automated decision making does not automatically entail the use of machine learning or artificial intelligence. However, this is generally the case in the current state of the security measures.[26] The sections in this chapter include first the technical aspects of the automated decision making linked to any legal implications (Section II.2.1). Afterwards, the options for decision making (Section II.2.2) come into play, as these are the ones producing legal effects on the individuals whose data was collected and processed.

Involvement of other entities in the decision-making process and/or the implementation of the decisions is included in Section II.2.3. The legal implications for using automated decision-making are further analysed and proposals for amendments are made in Section II.2.4. The

---

[20] Schmitt, Julia, Miller, Klaus M., Skiera, Bernd, The impact of privacy laws on online user behavior, Working paper, Goethe University Frankfurt, HEC Paris, 2020.

[21] Robinson, L., et al. Digital Inequalities 3.0: Emergent Inequalities in the Information Age, First Monday, vol. 25, no. 7, University of Illinois Libraries, 2020.

[22] Devlin, M. A., Hayes, B. P., Non-Intrusive Load Monitoring and Classification of Activities of Daily Living Using Residential Smart Meter Data, IEEE Transactions on Consumer Electronics, vol. 65, no. 3, pp. 339-348, Aug. 2019, doi: 10.1109/TCE.2019.2918922.

[23] Solove, Daniel J., Murky Consent: An Approach to the Fictions of Consent in Privacy Law, 104 Boston University Law Review (Forthcoming), GWU Legal Studies Thesis No. 2023-23, GWU Law School Public Law Thesis No. 2023-23, 2023, https://ssrn.com/abstract=4333743 or http://dx.doi.org/10.2139/ssrn.4333743.

[24] Moss, Emanuel, Watkins, Elizabeth, Singh, Ranjit, Elish, Madeleine Clare, Metcalf, Jacob, Assembling Accountability: Algorithmic Impact Assessment for the Public Interest, 2021, https://ssrn.com/abstract=3877437, last accessed on 28 August 2023.

[25] Hongbin, F., Zhi, Z. Privacy-Preserving Data Aggregation Scheme Based on Federated Learning for IIoT. Mathematics, vol. 11, pag. 214, 2023. https://doi.org/10.3390/math11010214

[26] Gibert, D., Mateu, C., Planes, J., The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. J. Netw. Comput. Appl., vol. 153, 102526, 2020.

anonymisation/pseudonymisation techniques and their legal and technical implications are included in Section II.2.5.

Chapter II.3 addresses to sub-objective 1.2, as it refers to active defence mechanisms that can be taken by the intermediary. [27] There are certain technical actions that can be taken by the intermediary at this stage.[28] However, under the current legislation, especially the data protection and criminal law legislation, there are certain limitations in this respect.[29] The types of actions that can be taken from a technical perspective and the limitations from a legal perspective are analysed in this chapter, together with anonymisation techniques that can mitigate certain legal concerns and risks.[30]

Hypothesis 1.2.1 refers to the possibility of intermediaries to take certain active steps at the moment when a potential breach of private life is identified.[31] One approach is to consider these actions as part of a self-defence steps taken by intermediaries on behalf of the victim (hypothesis 1.2.3). Further, after the active measures are taken, certain data pertaining to the potential cyber-attacker are obtained and there are certain limitations in terms of analysing this data, sharing it with other private entities and sharing it with public authorities (regulatory or criminal investigation bodies). Further, certain limitations in terms of public interest in view of maintaining order in terms of entities that have investigative powers.

Title III includes the analysis of existing obligations in relation to protection of private life pertaining to the intermediaries. It generally includes aspects relating to sub-objective 2.1 in the sense of proposing new legislation for proper preventive measures to be taken by the intermediaries to ensure security of the private life of their users. Such protection relates also to protection of devices and protection of data, as, in the digital environment these are interlinked.[32] Therefore, the criminal offence of illegal access to IT systems is closely linked to the criminal offence of breach of private life. [33] Further, the title includes also cooperation needs to achieve proper preventive security in an interconnected globalised ecosystem, in which threat intelligence is essential. In this respect, an outline of the main stakeholders is essential.[34]

The three main pillars for the obligations of intermediaries entail: legal obligations related to collection and processing of data pertaining to users, aspects to be analysed in terms of aggregation and sharing data and manner of determining the accountability of the intermediaries properly.[35] These three pillars represent the main vantage points to consider for analysis of existing

---

[27] Van Dijck, J., Governing digital societies: Private platforms, public values. Computer Law and Security Review, 36, p.105377, 2020.

[28] Rappaport, John, Some Doubts About 'Democratizing' Criminal Justice, The University of Chicago Law Review, vol. 87, no. 3, pp. 711–814, 2020, JSTOR, https://www.jstor.org/stable/26910603. Accessed 28 Aug. 2023.

[29] Cioclei, V., Drept penal, Partea speciala I, ed. a III-a, ed. C.H.Beck, pag 64, 2018.

[30] Hathaway, Oona et al., The Law of Cyber-Attack, California Law Review 100(4), 2011.

[31] Denning, Dorothy E., Framework and principles for active cyber defense, Computers and Security, vol. 40, pp. 108-113, 2014, https://doi.org/10.1016/j.cose.2013.11.004.

[32] Losavio, MM, Chow, KP, Koltay, A, James, J., The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security, Security and Privacy Journal. 2018.

[33] Zhou, G., Zhuge, J., Fan, Y. et al. A Market in Dream: the Rapid Development of Anonymous Cybercrime. Mobile Netw Appl 25, pp. 259–270, 2020, https://doi.org/10.1007/s11036-019-01440-2.

[34] Rana, Muhammad Usman, Ellahi, Osama, Alam, Masoom, Webber, Julian L., Mehbodniya, Abolfazl, Khan, Shawal, Offensive Security: Cyber Threat Intelligence Enrichment With Counterintelligence and Counterattack, IEEE Access, vol.10, pp.108760-108774, 2022.

[35] Cowls, Josh, Morley, Jessica, Floridi, Luciano, App store governance: Implications, limitations, and regulatory responses, Telecommunications Policy, vol. 47, Issue 1, 2023, https://doi.org/10.1016/j.telpol.2022.102460.

obligations and need for additional new obligations, while the following chapter IV will analyse limitations in existing legislation for implementing such obligations properly.

Chapter III.1 focuses on the obligation that are currently in place and those than can be set in place for intermediaries, based on the role thereof, as analysed and detailed in this thesis.[36] To this end, the chapter analyses the security requirements for collection of data, the obligations about ensuring security requirements are in place and the cyber-attack types that can be identified and analysed by intermediaries. Further, it analyses in cooperation with other entities within the digital ecosystem and correlation with other relevant criminal offences under which the actions of the intermediaries can be considered criminal actions unless specific legislation is set in place.[37] This entails that further legislative steps have to be taken in order for the preventive security actions of the intermediaries not to be considered criminal offences themselves, especially in terms of the breach of private life of the users they are protecting from cyber-attacks.[38] This chapter also includes an overview of the policies and procedures made public by the intermediaries in terms of the security measures they have implemented under the current legislation and without specific legal requirements in this respect, but with the view of protecting their users as much as possible.[39]

Chapter III.2 focuses on the manner to implement the obligation of the intermediaries proposed in this thesis to ensure proper preventive measures. The chapter analyses the manner in which the intermediaries can aggregated data and share it in order to enhance their accuracy of identification of cyber-attack, cyber-attack patterns and exploitable vulnerabilities and exploitable misconfigurations.[40] To this end, the chapter includes aspects pertaining to sharing raw data or results of analysis by the intermediaries to other entities (including other intermediaries and authorities) and also the aggregation of data at the level of the user or at the level of all users of the intermediary.[41] In addition, the usefulness of anonymisation and pseudonymisation is included in this chapter as a manner of complying with data protection and criminal legislation, as well as ensuring security of data collected.

Chapter III.3 includes details on how to establish the accountability of the intermediaries.[42] It includes accountability aspects in current data protection, human rights and criminal legislation and it further analyses the legal concerns based on types of attacks and based on the type of response to such attacks.[43] The accountability of the intermediaries is further analysed in terms of periodic review on the intermediary's activity, its just-in-time implementation of security measures and proper documentation of security measures taken and reasoning for choosing such security measures.

---

[36] Pistor, Katharina, Rule by Data: The End of Markets?, 83 Law and Contemporary Problems, pp. 101-124, 2020.

[37] Gasser, Urs and Schulz, Wolfgang, Governance of Online Intermediaries: Observations from a Series of National Case Studies, 2015. Berkman Center Research Publication No. 2015-5, https://ssrn.com/abstract=2566364 or http://dx.doi.org/10.2139/ssrn.2566364.

[38] Daniel, L.E., Digital forensic for legal professionals. Understanding digital evidence from the warrant to the courtroom, 1st ed., ed. Syngress, pag. 124, 2011.

[39] Gasser U, Schulz W., Governance of Online Intermediaries – Observations From a Series of National Case, 2015, https://ssrn.com/abstract=2566364, last accessed on 29 August 2023.

[40] Moura, José, Serrão, Carlos, Security and Privacy Issues of Big Data, part of Handbook of Research on Trends and Future Directions in Big Data and Web Intelligence, 2015.

[41] Corwin, EH. Deep packet inspection: Shaping the Internet and the implications on privacy and security, Information Security Journal: A Global Perspective, vol. 20(6):311-6., 2011.

[42] Shi, L, Li, K. Privacy Protection and Intrusion Detection System of Wireless Sensor Network Based on Artificial Neural Network, Computer Intelligence Neuroscience, vol. 2022:1795454, 2022, doi: 10.1155/2022/1795454.

[43] Alotaibi, Saud, et al., A novel behaviour profiling approach to continuous authentication for mobile applications, SCITEPRESS-Science and Technology Publications, 2019.

Chapter III.1 analyses the current obligations under Romanian law that can lead to an interpretation that intermediaries have obligations to guard private life of the users and proposals to adjust such obligations to reflect the current role of entities within the digital ecosystem.[44] The intermediaries are positioned in a manner at the core of most of the activities performed by users on their devices, having an overview of the entire ecosystem of applications and internet destinations used by the users. [45]

Under current legislation, as shown in this research, there are no legal obligations to implement preventive security measures.[46] While there are obligations for specific entities to implement certain security preventive measures within their organisation or within the software they provide to customers, intermediaries are not covered by such obligations and, further, the intrusion detection and prevention approach analysed in this thesis is not covered under existing legislation. The chapter focuses on sub-objective 2.1, respectively, hypothesis 2.1.1 that refers to the need for additional legal obligations of the intermediaries in order to prevent breaches of life, as this term has been defined under existing legislation and the proposed changes mentioned in Title II above.

Thus, this chapter emphasizes indirectly the usefulness of adding certain criminal law adjustments to the concept of private life, in order to reflect the digital landscape. This would bring the concept of private life and the criminal law manner of protection in line with the digitalisation currently covering the activities and life of the users.[47] Further, in case of inaction with intent to ensure proper security measures, similar criminal liability should be triggered, as it indirectly helps the perpetrators commit the breach of private life criminal offence.[48] This entails that, even under the current protection of private life, intermediaries' obligations proposed in this thesis are actually required, as, any inactivity in this respect can result in the breach of private life of the users.[49]

Two other sub-objectives are addressed in this chapter in terms of cooperation, sub-objective 2.2, with hypothesis 2.2.3 (technical limitations for implementing security measures that are dependent on other entities) and hypothesis 2.1.3 (cooperation between digital stakeholders to ensure swift and effective implementation of preventive security measures).[50]

The chapter focuses first on the legal basis and legal requirements for collection of data about the user.[51] This entails an overview of data protection and criminal law aspects. Further, such requirements are placed within the digital legislation ecosystem and other criminal offences

---

[44] Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies).

[45] Zhang, Lei, Yang, Zhemin, He, Yuyu, Li, Mingqi, Yang, Sen, Yang, Min, Zhang, Yuan, Qian, Zhiyun, App in the Middle: Demystify Application Virtualization in Android and its Security Threats. Proc. ACM Meas. Anal. Comput. Syst. 3, 1, Article 17, 2019, https://doi.org/10.1145/3322205.3311088.

[46] Harkin, D., Molnar, A., Operating-System Design and Its Implications for Victims of Family Violence: The Comparative Threat of Smart Phone Spyware for Android Versus iPhone Users. Violence Against Women, vol. 27(6–7), pp. 851–875, 2021. https://doi.org/10.1177/1077801220923731.

[47] Zhou, G., Zhuge, J., Fan, Y. et al. A Market in Dream: the Rapid Development of Anonymous Cybercrime. Mobile Netw Appl 25, pp. 259–270, 2020, https://doi.org/10.1007/s11036-019-01440-2.

[48] Almomani, I. M., Khayer, A. A., A Comprehensive Analysis of the Android Permissions System, in IEEE Access, vol. 8, pp. 216671-216688, 2020, doi: 10.1109/ACCESS.2020.3041432.

[49] Zhou, G., Zhuge, J., Fan, Y. et al. A Market in Dream: the Rapid Development of Anonymous Cybercrime. Mobile Netw Appl 25, pp. 259–270, 2020, https://doi.org/10.1007/s11036-019-01440-2.

[50] Araba Vander–Pallen, M., Addai, P., Isteefanos, S., Khan Mohd, T., Survey on Types of Cyber Attacks on Operating System Vulnerabilities since 2018 onwards, 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 2022, pp. 01-07, doi: 10.1109/AIIoT54504.2022.9817246.

[51] Pistor, Katharina, Rule by Data: The End of Markets?, 83 Law and Contemporary Problems, pp. 101-124, 2020.

regulated under the criminal law than the breach of private life that may be relevant in the digital environment and for the protection of the private life of users.[52] Further, from a practical technical perspective, the requirement identified in the chapter are mapped to the types of attacks to be identified and analysed by the intermediaries and the correlation from a technical perspective with the other stakeholders within the digital ecosystem.[53] The chapter also includes a case study to analyse the manner in which a set of intermediaries handle security of their users at present, by reference to the obligations they undertake in the publicly available terms and conditions.[54]

Chapter III.2 analyses one of the most important activities in terms of security prevention, respectively, the collection and analysis of data from multiple users and in the context of aggregation of data. The collection can be performed by the intermediary itself or from other intermediaries or third parties. The chapter includes analysis from multiple legislative and practical perspectives, including data protection and criminal law.[55]

The approaches that can be taken in practice include aggregation of data from multiple devices and multiple users. This gives the overview on the typologies of cyber-attackers and gives more insights into the attack vectors used, especially for malicious links sent in chats and phishing/vishing attempts.[56] Aggregated data ensures from a statistical and probability perspective, a more accurate view on the user landscape and on the cyber-threat overview. Further, such increased amount of data is important for any machine learning and artificial intelligence algorithms used by the intermediaries in view of training such algorithms in order to obtain a more accurate result.[57]

Subsequently, it is essential to understand the sharing legal limitations in order to frame the legal obligation of intermediaries properly and to distinguish between the liability of intermediaries and liability of other entities/users. The sharing of data analysed includes that towards and from authorities, other intermediaries and other entities within the digital ecosystem. It also analyses sharing of raw data and of results of analysis performed by any of such entities.[58]

This chapter focuses on sub-objective 1.1 and, more specifically, on hypothesis 1.1.2 and hypothesis 1.1.3. Hypothesis 1.1.2 refers to the limitations that exist in terms of aggregation of data and hypothesis 1.1.3 on the use of anonymisation and pseudonymisation techniques for analysis of aggregated data. Thus, the chapter includes details on the approach to be taken to maximize the aggregation and sharing data without negatively affecting the private life of the

---

[52] Tremolada, R., Common carriers and public utilities in the digital ecosystem: Unravelling the taxonomy on a quest for better regulation. Information and Communications Technology Law, vol. 31(1), pp.35-80, 2022.

[53] Diaconu, D.V., Supravegherea video, audio sau fotografierea si patrunderea in spatii private.

[54] Dieter, M., Gerlitz, C., Helmond, A., Tkacz, N., van Der Vlist, F.N., Weltevrede, E., Multi-situated app studies: Methods and propositions. Social Media+ Society, vol. 5(2), p.2056305119846486, 2019.

[55] Back, S., LaPrade, J., Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions. International Journal of Cybersecurity Intelligence and Cybercrime, vol. 3(2), pp. 25-47, 2020, https://www.doi.org/10.52306/RGWS2555.

[56] Breen, Casey, Herley, Cormac, Redmiles, Elissa M., A Large-Scale Measurement of Cybercrime Against Individuals, Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22). Association for Computing Machinery, New York, NY, USA, pp. 1–41, 2022, https://doi.org/10.1145/3491102.3517613.

[57] Moura, José, Serrão, Carlos, Security and Privacy Issues of Big Data, part of Handbook of Research on Trends and Future Directions in Big Data and Web Intelligence, 2015.

[58] Garg, Shivi, Baliyan, Niyati, Data on Vulnerability Detection in Android, Data in Brief, vol. 22, pp. 1081-1087, 2019, https://doi.org/10.1016/j.dib.2018.12.038.

users, while leveraging the anonymisation and pseudonymisation mechanisms which are appropriate from a business and privacy perspective.[59]

Chapter III.3 aims to setup proper proposals for ensuring security preventive measures are taken by the intermediaries. In doing so, it takes into account the intrusiveness aspects established in chapter II with respect to the data and private life of users and of cyber-attackers and makes proposals for technical and organisational security measures that can be taken by intermediaries. The chapter also takes into account the other legal provisions concerning preventive security measures in the digital ecosystem.[60] The focus is on the practical steps that can be taken by the intermediaries, the timing for such actions and whether these are already covered by existing legislation or they should be further specified in specific legislation. To this end, the approach taken is that of having a real-time response by the intermediaries based on the information they hold at a certain point in time.[61] This concept has been analysed in legislation previously in the context of user-facing applications in the payments services directive 2, Directive (EU) 2015/2366 on payment services in the internal market and article 18 of Commission delegated regulation (EU) 2018/389 supplementing PSD2 of 27 November 2017, which goes into detail also with certain aspects to analyse (abnormal behavioural pattern of the user, malware infection, abnormal location, high-risk location).

The chapter focuses on sub-objective 2.1, with emphasis on hypothesis 2.1.1 and 2.1.2, as it establishes the as-is situation in terms of legal obligations of the intermediaries, it further identifies situations in which the intermediaries are best placed to address a certain security concern and includes proposals for preventive steps that intermediaries can take. For this purpose, the chapter analyses the types of technical measures that can be taken by the intermediaries and the manner in which these can be addressed through the existing legislation, as well as proposed new legal requirements.[62]

Title IV includes analysis of limitations to actions of intermediaries for preventing breaches against the private life of users. To this end, we first analyse the proposed legal requirements for intermediaries in view of collecting data, analysing data and sharing data in view of ensuring that preventive security measures are in place.[63] Secondly, we analyse the technical capabilities of intermediaries, given the data to which they have access and the control/permissions they have over the device/accounts of the user. The technical limitations translate into legal limitations and limitations of liability of intermediaries.[64] Having such matters clearly established from the outset reduces litigation for clarifications afterwards. Subsequently, based on such limitations, this title details proposed changes to existing data protection and criminal law legislation in view of

---

[59] Solove, Daniel J., The Myth of the Privacy Paradox, 89 George Washington Law Review 1, GWU Legal Studies Thesis No. 2020-10, GWU Law School Public Law Thesis No. 2020-10, 2021, https://ssrn.com/abstract=3536265 or http://dx.doi.org/10.2139/ssrn.3536265

[60] Bank, David, Yamin, Dan, Predicting Cyber-Infections Via Web-Browsing Patterns, 2020, https://ssrn.com/abstract=3757877 or http://dx.doi.org/10.2139/ssrn.3757877.

[61] Khan, Minhaj Ahmad, A survey of security issues for cloud computing, Journal of Network and Computer Applications, vol. 71, pp. 11-29, 2016, https://doi.org/10.1016/j.jnca.2016.05.010.

[62] DeNardis, L., Musiani, F., Governance by infrastructure. In The turn to infrastructure in Internet governance, pp. 3-21, New York: Palgrave Macmillan US, 2016.

[63] Folino, Gianluigi, Sabatino, Pietro, Ensemble based collaborative and distributed intrusion detection systems: A survey, Journal of Network and Computer Applications, Vol. 66, pp. 1-16, 2016, https://doi.org/10.1016/j.jnca.2016.03.011.

[64] Haelterman, Harald, Situational crime prevention and supply chain security: an "Ex Ante" consideration of preventive measures, Journal of Applied Security Research 4, no. 4, pp. 483-500, 2009.

overcoming such limitations and ensuring possibility of security measures ensured by the intermediaries and, at the same time, limits to the types of security measures that can be taken.[65]

Chapter IV.1 analyses the legal limitations under criminal law, human rights and data protection with respect to actions that can be taken by intermediaries to prevent breaches of private life of users.[66] These limitations occur due to the need for access to certain IT systems and to data of the users in order to create and implement appropriate preventive security measures. Further, the legal limitations relate to the fact that certain actions that can be performed by the intermediaries can have an impact from a private life criminal offence perspective or on the IT systems used by the user.[67] Additional complications to the legal analysis relate to the situation whereby the device used by the user is used by other individuals as well or in situations whereby the device used by the user contains data pertaining to the private life of other individuals as well. In addition, there are certain legal steps that can be taken by the intermediary to avoid liability given the technical constraints in taking actions after they perform the data analysis.

Chapter IV.2 is aimed at building on the legal limitations and recommendations from the above chapter IV.1 and highlighting the technical limitations. These limitations can stem firstly from the pure technical limitations of security at present and limitations from the side of the devices from a technical perspective (as detailed under section IV.2.1). Specific limitations may arise in terms of analysis of traffic data from or to the device of the user (as detailed under section IV.2.5) and vulnerabilities of other applications or other intermediaries (as detailed under section IV.2.4).[68] One approach to address this wide landscape is setting-up standards and best practices (as detailed under section IV.2.3). This provides clarity on the legal obligations of each stakeholder and on the level of security controls to be implemented. Secondly, they can stem from the technical limitations due to dependencies on other entities in the digital ecosystem[69] (as detailed under section IV.2.2). Thirdly, the performance aspect should also be had in mind, as security tools can have a high impact on the performance of the hardware and software within the device of the user (as detailed under section IV.2.6).[70]

This chapter is related to two sub-objectives. It details certain points concerning sub-objective 2.1 in relation to hypothesis 2.1.3 on cooperation being a requirement for ensuring proper prevention. In terms of sub-objective 2.2, the chapter touches upon hypothesis 2.2.3 in the sense that it includes certain technical limitations that have to be had in mind when assessing the obligation of intermediaries to prevent breaches of private life and upon hypothesis 2.2.4 in terms of the performance limitations that also reduce the types of security measures that can be taken on

---

[65] Tatar, Unal, Gokce, Yasir, Nussbaum, Brian, Law versus technology: Blockchain, GDPR, and tough tradeoffs, Computer Law and Security Review, vol. 38, 2020.

[66] Cath, C., The technology we choose to create: Human rights advocacy in the Internet Engineering Task Force. Telecommunications Policy, 45(6), p.102144, 2021.

[67] Zlati, G., Legitima aparare si starea de necessitate in domeniul criminalitatii informatice, Dreptul, 4/2015, 2015.

[68] Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., Bulakh, V., Decrypting SSL/TLS traffic for hidden threats detection, 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 143-146, 2018, doi: 10.1109/DESSERT.2018.8409116.

[69] Karagiannis, C. Digital evidence “hidden in the Cloud”: Is “possession” still a relevant notion?. ERA Forum 23, pp. 301–311, 2023. https://doi.org/10.1007/s12027-022-00724-7

[70] Madala, Ravikiran, A Novel Dynamic Watermarking for Secure Data Protection from Cyber Theft Based on Artificial Intelligence Supervision, 2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), 2023, https://ssrn.com/abstract=4475548.

a particular device.[71] In essence, all such technical or organisational limitations have an impact on the number of successful breaches to private life of users and should be clearly identified to prevent civil, administrative or criminal liability of intermediaries for not preventing them, as detailed below.

The research includes the analysis of EU level legislation and Romanian law legislation concerning criminal law, data protection and human rights. Other angles are also relevant, for example, competition law and consumer protection. However, these are not the focus of this research. In addition, the research focuses on the above two objectives in terms of identifying the role of intermediaries in preventing potential criminal offences while not partaking in criminal actions themselves.[72] This research results in a set of proposed legal provisions in this respect. Such proposals are validated also through a quantitative approach. Nevertheless, additional validation of the impact assessment of such proposals can be performed, including their impact from other perspectives than the criminal law, data protection and human rights law.[73]

We are outlining below a couple of angles of the private life concept not included in this thesis and which can be topics of future research in this field:

- Data analytics (especially in the big data context), together with any profiling or tracking activities and any automated decisions concerning individuals (which may create legal consequences or similar effects on individuals).[74]
- Consumer protection (including specific requirements concerning children)[75] and competition law implications in case of sharing of data.[76]
- Specifics for data sharing in case of a relation between employer and employee, including aspects relating to monitoring of employees' online activity.
- Remedies for harms brought by privacy infringements, including damages paid to individuals or to other companies on the basis of tort or contractual liability (including cyber insurance claims). The ECHR[77] has defined broadly the concept of private life (which has

---

[71] Zhou, Chenfeng Vincent, Leckie, Christopher, Karunasekera, Shanika, A survey of coordinated attacks and collaborative intrusion detection, Computers and Security, vol. 29, Issue 1, pp. 124-140, 2010, https://doi.org/10.1016/j.cose.2009.06.008.

[72] Slavoiu, Radu, Protectia penala a vietii private, Universul Juridic, pag. 138, 2016.

[73] Bianchi, G. et al., Towards Privacy-Preserving Network Monitoring: Issues and Challenges, 2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, Athens, Greece, pp. 1-5, 2007, doi: 10.1109/PIMRC.2007.4394186.

[74] EDPS, Leading by Example: The EDPS Strategy 2015-2019, pag. 17. 'Big data,' in our view, 'refers to the practice of combining huge volumes of diversely sourced information and analysing them, often using self-learning algorithms to inform decisions. One of the greatest values of big data for businesses and governments is derived from the monitoring of human behaviour, collectively and individually, and resides in its predictive potential; EDPS Opinion 4/2015, Towards a new digital ethics: Data, dignity and technology, 2015. EDPS, Opinion 7/2015 Meeting the challenges of big data, 2015. EDPS, Opinion 8/2016 Opinion on coherent enforcement of fundamental rights in the age of big data, 2016.

[75] U.S House of Representatives Committee on Energy and Commerce, hearing entitled 'Algorithms: How Companies' Decisions About Data and Content Impact Consumers' 2017, http://docs.house.gov/meetings/IF/IF17/20171129/106659/HHRG-115-IF17-20171129-SD002.pdf, last accessed on 24 December 2022. The Department of Commerce, Internet Policy Task Force, Cybersecurity, Innovation and the Internet Economy, 2011.

[76] Goldfarb, Avi and Tucker, Catherine, Privacy and Innovation, 12 INNOVATION POL'Y and ECON. 65, 2012.

[77] ECHR, Klass and Others v. Germany, case no. 5029/71, para. 55-60, Von Hannover v. Germany case no. 40660/08 and 60641/08, para. 50-53, Sciacca v. Italy, case no. 50774/99, para. 27-30, Rotaru v Romania case no. 28341/95,

some ties with the privacy and personal data concepts), including any information about private and family life, residence, correspondence (email, telephone, workplace email).[78]

Further, the prevention legal obligations should include both criminal law and civil law considerations. In addition, these should reflect and should be interpreted by the courts of law in light of the technical limitations and the technical capabilities related to such situations. In this decade, de legislation has been developing in order to catch up with the continuously changing technological landscape.

The legislation has focused significantly on internal organisation of entities in view of implementing proper security best practices and also on the secure software development lifecycle. For this reason, we have chosen to focus on an existing gap in the existing legislation, respectively, the role of intermediaries in ensuring preventive security measures in view of protecting the private life of the individuals using the services of the intermediary.

In view of showing the usefulness of having legal obligations for intermediaries within a certain activity, we have looked at the anti-money laundering legislation which has placed over the years more and more obligations on the intermediaries of the money laundering transactions, including banks, etc. Thus, in view of detecting such criminal offences and, subsequently, in order to ensure preventive measures against them, the legislator has opted to have obligations based on the intermediaries involved in the ecosystem.[79]

---

para. 59-60; P.G. and J.H. v the UK case no. 44787/98, para. 61-63; Peck v. UK case no. 44647/98, para. 102-104; Amann v. Switzerland case no. 27798/95, para. 75-80.

[78] Duca, Maria Violeta, Răspunderea patrimonială a angajatorului. Supravegherea nelegală a modalităţii de utilizare a laptopului şi telefonului de serviciu. Daune morale pentru intruziunea în viaţa privată a salariaţilor, Revista Romana de Jurisprudenta 2/2018, 2018. Bucharest Court of Appeal, decision no. 3033/2018.

[79] Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries adopted by the Council of Europe in April 2018.