LARISA GĂBUDEANU

CYBER DEFENCE PROTECTION OF PRIVATE LIFE PERFORMED BY INTERMEDIARIES

Universul Juridic
București
-2025-

Cuprins

Title I

Introduction and overview of preventive measures for protection of data

This title includes the preliminary aspects concerning the scope of the research, the reasoning for choosing this topic for research and the gaps identified in literature review. Further, the research objectives and methodology are included herein. This sets the overview for the subsequent titles that analyse in depth the proposed objectives and the related hypotheses.

❍ Chapter I.1 Introduction

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-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

---

[1] Capgemini, Global non-cash transaction volumes, 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.

[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.

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 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.