

LARISA GĂBUDEANU

**CYBER DEFENCE PROTECTION  
OF PRIVATE LIFE PERFORMED  
BY INTERMEDIARIES**

**Universul Juridic**  
București  
-2025-

CUVÂNT ÎNAINTE – Conf. univ. dr. Laura Maria Stănilă .....	7
FOREWORD – Conf. univ. dr. Elena Lazăr .....	9
<b>TITLE I. INTRODUCTION AND OVERVIEW OF PREVENTIVE MEASURES FOR PROTECTION OF DATA .....</b>	<b>11</b>
Chapter I.1 Introduction.....	11
Chapter I.2 Research objectives and methodology .....	16
Section I.2.1 Research objectives.....	19
Section I.2.2 Research methodology.....	20
Section I.2.3 Limitations of research.....	24
Section I.2.4 Motivation of subject chosen .....	25
Chapter I.3 Current status of literature and identification of research gap.....	28
Section I.3.1 Private life in European legislation .....	32
A. Criminal law view.....	32
B. Human rights view.....	33
C. Data protection view.....	34
Section I.3.2 Digitalisation’s impact on the concept of private life.....	35
A. Digital private life.....	35
B. Large number of stakeholders.....	36
C. Data security landscape.....	40
Section I.3.3 Concept of intermediaries in European legislation.....	44
A. Essential service providers.....	45
B. Manufacturing providers.....	46
C. Platforms .....	46
Section I.3.4 Active players in the perpetration of criminal offences against private life .....	47
A. Cyber-attackers targeting certain applications used by the user .....	48
B. Cyber-attackers targeting identify theft.....	49
C. Cyber-attacker targeting extortion or damages.....	49
Section I.3.5 Active players in the prevention of criminal offences against private life.....	50
A. Application providers.....	51
B. Authorities.....	51
C. Users.....	52
<b>TITLE II. CORRELATION BETWEEN INTRUSIVENESS IN PRIVATE LIFE IN THE CRIMINAL LAW AND PRIVACY LEGISLATION IN THE CONTEXT OF SECURITY MEASURES.....</b>	<b>54</b>
Chapter II.1 Interplay between intrusiveness under criminal law and under privacy legislation.....	54
Section II.1.1 Concept of intrusiveness and private life.....	54
A. Concept of intrusiveness under data protection legislation .....	60
B. Concept of private life under criminal law.....	61
C. Concept of private life under human rights legislation .....	66
Section II.1.2 Data of individuals covered by private life.....	66
A. Current criminal law view .....	67
B. Current data protection view.....	67

C. Current human rights view.....	68
D. Comparative legislation view.....	68
E. Proposed view.....	70
F. Limitations given new technologies (cloud, blockchain, IoT, metaverse).....	70
G. Implication of the IT system concept in criminal law on data definition.....	71
Section II.1.3 Validity of victim's consent under criminal law.....	72
A. Validity of consent expressed.....	72
B. Moment of issuing the consent.....	73
C. Role of the consent in the perpetration of the criminal offence.....	73
Section II.1.4 Privacy harm categories and their role in criminal law interpretation.....	74
Section II.1.5 Digital private life specifics.....	77
A. Location of data.....	77
B. Format of data.....	78
C. Location of user.....	78
D. Location of user's device.....	79
Section II.1.6 Results of the questionnaire concerning the concept of intrusiveness in the context of security mechanisms.....	80
Section II.1.7 Legal provision proposals.....	85
Section II.1.8 Conclusions.....	86
Chapter II.2 Use of automated decision making in the security prevention mechanism on data subject to the data minimisation principle.....	88
Section II.2.1 Technical usefulness of automated decision making.....	88
A. Real-time analysis across multiple users.....	88
B. Real-time actions taken by intermediaries.....	91
C. Real-time interaction with users.....	92
D. Computer performance aspects.....	93
Section II.2.2 Implications for decision making.....	94
A. Stop.....	95
B. Notify.....	96
C. Confirm.....	97
Section II.2.3 Involving other entities from the digital ecosystem in the decision- making process.....	98
A. Requesting specific data from other entities.....	98
Section II.2.5 Anonymisation/pseudonymisation of data.....	109
A. Concept of personal data and relevance of un-anonymised data usage.....	109
B. Types of anonymisation/pseudonymisation techniques.....	112
Section II.2.6 Results of the questionnaire concerning automated decision making for securing private life.....	118
Section II.2.7 Legal provision proposals.....	123
Section II.2.8 Conclusions.....	125
Chapter II.3 Using active defence mechanisms as prevention mechanisms and legal implications thereof.....	129
Section II.3.1 Obligation of active prevention steps and immediate intervention in case breach identification.....	129
A. Active actions of intermediaries in case of private life breach.....	130
B. Reconnaissance for future blocking of data accessing/leaking.....	133
Section II.3.2 "Without right" data collection, analysis and transfer.....	134
A. Limitations to the concept of "without right" in case of perpetrator data.....	134
B. Transparency toward perpetrators.....	139
Section II.3.3 Perpetrator data analysis.....	140

A. Gathering and correlating data of perpetrators .....	140
B. Sharing data .....	141
C. Making data publicly available .....	143
D. Bots use case .....	143
Section II.3.4 Active defence through honeypots .....	145
A. Criminal law implications .....	145
B. Data protection implications .....	151
Section II.3.5 Self-defence (intermediaries on behalf of individuals) .....	152
A. Concept of self-defence in the context of the private life beach criminal offence .....	152
B. Actions that can be taken as self-defence .....	154
C. Self-defence subject .....	156
Section II.3.6 Necessity state .....	157
A. Concept of necessity state in the context of the private life beach criminal offence .....	157
B. Actions that can be taken as necessity state .....	158
C. Necessity state subject .....	159
Section II.3.7 Sharing data of potential cyber-attacker .....	159
A. Criminal law implications for sharing data pertaining to the cyber-attacker .....	160
B. Data protection law implications .....	161
C. Human rights implications .....	162
Section II.3.8 Results of the questionnaire concerning active defence performed by intermediaries .....	162
Section II.3.9 Legal provision proposals .....	165
Section II.3.10 Conclusions .....	167

**TITLE III. BALANCING RIGHTS AND OBLIGATIONS OF INTERMEDIARIES IN GUARDING THE PRIVATE LIFE THROUGH PREVENTIVE MECHANISMS .....**

Chapter III.1 Obligations of intermediaries to guard private life .....	173
Section III.1.1 Legal basis for collection of data about the user .....	174
A. Consent .....	175
B. Legitimate interest .....	177
C. Public interest .....	179
D. Legitimate self-defence and necessity state .....	180
Section III.1.2 Legal requirements for collection of data .....	181
A. Transparency .....	181
B. Retention period for data .....	183
C. Moment of accessing – data minimisation .....	184
D. Data subject rights .....	184
Section III.1.3 Correlation of data collection right with other relevant legislation for protection of data/IT systems .....	186
A. Payment Services Directive 2 – PSD2 .....	186
B. Network Information Security Directive – NIS and NIS 2.0 Directives .....	187
C. Romanian security measures for financial services .....	188
D. Digital Operational Resilience Act – DORA .....	188
E. Draft Cyber resilience Act and Product Liability Directive .....	189
F. Draft Artificial Intelligence EU legislation .....	189
Section III.1.4 Correlation with other criminal offences .....	190
A. Breach of domicile .....	190
B. Breach of correspondence .....	191
C. Deceit .....	194

D. Correlation with illegal access to IT system or illegal transfer from IT system .....	195
Section III.1.5 Types of attack techniques to be analysed by intermediaries.....	196
A. Malware, crime as a service and script kiddies.....	197
B. Man in the middle attack.....	205
C. Authentication and authorisation attacks.....	206
D. Device used as part of a botnet.....	207
E. Phishing and vishing.....	208
Section III.1.6 Existence of multiple entities involved in the data storage/processing.....	209
A. Relevance of access to data to ensure security of data .....	210
B. Correlation of multiple layers of defence needing data from multiple layers .....	211
C. User's responsibility .....	211
D. Responsibility of application providers and platform providers.....	213
Section III.1.7 Case studies – terms and conditions of intermediaries.....	214
A. Operating system .....	214
B. Browser .....	217
C. Application store .....	220
Section III.1.8 Results of the questionnaire concerning obligations of intermediaries .....	222
Section III.1.9 Legal provision proposals.....	224
Section III.1.10 Conclusions.....	227
Chapter III.2 Rights of intermediaries in aggregation and sharing of data while abiding to their privacy requirements.....	233
Section III.2.1 Implications in aggregating data at the level of the intermediary.....	233
A. Aggregating data from a user on multiple devices.....	234
B. Aggregating data from multiple users .....	237
C. Criminal offence of data transfer without right for aggregated data.....	239
Section III.2.2 Sharing data to other intermediaries .....	240
A. Sending raw data directly to other intermediaries .....	243
B. Sending analysis to other intermediaries .....	244
C. Regulating the retention period and purpose of processing .....	245
Section III.2.3 Sharing data to authorities.....	247
A. Possibility of intermediaries to file complaints with authorities on behalf of users.....	248
B. Sharing raw data directly to authorities.....	250
C. Sharing analysis results with authorities.....	251
D. Onward transfer situations and purpose of transfer limitation .....	252
Section III.2.4 Sharing data to other entities having security prevention obligations .....	253
B. Sharing analysis result.....	258
C. Performing actions to ensure security of user's private life on behalf of these entities .....	259
Section III.2.5 Obtaining data analysis results from other entities (e.g. intermediaries, authorities, entities having security prevention obligations) .....	260
A. Accuracy of data and implications for the security prevention .....	260
B. Liability of inaccurate data analysis results.....	261
C. Direct or indirect contractual relations for obtaining data analysis results.....	263
Section III.2.6 Roles of anonymisation/pseudonymisation in pattern identification.....	264
A. Role of the collecting entity.....	264
B. Role of the data analysis result sharing entity.....	265
C. Role of the data analysis entity .....	266
Section III.2.7 Results of the questionnaire concerning data aggregation and data sharing by intermediaries .....	268

Section III.2.8 Legal provision proposals .....	270
Section III.2.9 Conclusions .....	272
Section III.3.1 Current legal basis for taking preventive security measures .....	276
A. Criminal law .....	276
B. Data protection .....	281
C. Current proposals at EU level for security prevention mechanisms .....	285
Section III.3.2 Legal concerns for technical angles for preventive security measures .....	288
A. Misconfiguration-alerts for misconfiguration of user accounts (e.g. app, cloud) .....	288
B. Vulnerabilities identified by the intermediary .....	289
C. Inclusion of the user's device in a bot network .....	289
D. Keyloggers .....	290
E. Remote access applications .....	290
F. Data exfiltration malware .....	291
G. Ransomware .....	291
Section III.3.3 Legal implications of actions to be taken by intermediaries .....	292
A. Updates or configurations not performed by the user .....	293
B. Automatic push of updates and security measures .....	294
C. Prohibition to use certain services until the update is complete .....	295
D. Negligence of user when approving actions .....	296
E. Lack of proper identification of cyber-attacks .....	297
F. False positives identified .....	298
G. Lack of data to clearly identify cyber-attacks .....	299
Section III.3.4 Periodic security reviews .....	300
A. Periodic scanning the device for malware, etc .....	301
B. Periodic vulnerability scanning on the user's device .....	301
C. Periodic auditing .....	302
D. Periodic certification .....	302
Section III.3.5 Just-in-time security measures .....	303
A. Just-in-time analysis of interactions with the intermediary's software .....	303
B. Just-in-time analysis of actions taken by the user's device .....	304
C. Just-in-time analysis of the actions taken by the user .....	305
Section III.3.6 Technical documentation of security prevention analysis and decision-making process .....	306
A. Algorithm decision making process .....	306
B. Decisions and actions taken for each user .....	307
Section III.3.7 Results of the questionnaire concerning accountability of intermediaries .....	308
Section III.3.8 Legal provision proposals .....	314
Section III.3.9 Conclusions .....	316

TITLE IV. LIMITATIONS IN PREVENTION MECHANISMS ENSURED BY INTERMEDIARIES .....	321
Chapter IV.1 Legal limitations to actions of intermediaries .....	321
Section IV.1.1 Data protection implications .....	321
A. Limitations in terms of monitoring activities .....	322
B. Limitations in terms of processing basis and constraints .....	327
Section IV.1.2 Human rights implications .....	332
A. Limiting information gathering .....	332
B. Concept of new technologies in the view of the ECHR .....	334
Section IV.1.3 Technical limitations to incrimination of intermediaries' actions .....	336

A. Avoiding damages to users.....	336
B. Avoiding breach of private life.....	338
C. Contractual provisions with other entities in the ecosystem.....	339
Section IV.1.4 Consent of the victim.....	340
A. Scope of consent relevant to maintain the security measures .....	341
B. Validity of consent given by the injured individual .....	342
C. Withdrawal of consent.....	346
Section IV.1.5 Exemption from violation of private life .....	347
A. The breach of private life occurs to prevent a criminal offence.....	347
B. Public interest of the community.....	348
C. Participator at the video/image/voice communication .....	350
D. The victim acted intentionally to be seen by third parties.....	351
Section IV.1.6 Results of the questionnaire concerning legal limitations for intermediaries implementing prevention mechanisms.....	352
Section IV.1.7 Legal provision proposals .....	355
Section IV.1.8 Conclusions.....	357
Chapter IV.2 Technical limitations that influence the legal requirement of prevention .....	360
Section IV.2.1 Limitations of technical mechanisms for prevention .....	361
A. Strong customer authentication.....	362
B. Just-in-time authentication and authorisation .....	363
C. Limited authorisation for background applications.....	363
D. User-app profile anomaly detection.....	364
E. Traffic filtering for web browsing.....	364
F. Authentication of server .....	365
G. Hash to ensure integrity of files.....	365
H. Data stored outside the device (e.g. cloud, blockchain, metaverse, IoT) .....	365
I. Email correspondence and similar messages (e.g. chats) .....	366
J. Microphone and video access .....	366
Section IV.2.2 Dependence on other entities in the digital ecosystem for obtaining data .....	367
A. Stakeholders in the digital ecosystem and their role for securing private life of users.....	367
B. Legal requirements adjustment .....	376
C. Contractual structure with intermediaries.....	377
Section IV.2.3 Using cyber-attack patterns for threat prevention.....	378
A. Applying cyber-attack patterns to activity of user.....	379
B. Best practices for web applications/mobile applications as a security by design principle .....	380
Section IV.2.4 Vulnerabilities of other applications/components.....	381
A. Notification of users.....	382
B. Cooperation with other application producers.....	384
C. Blocking of certain applications .....	386
Section IV.2.5 Traffic data analysis.....	388
A. Access to encrypted traffic.....	388
B. Unencrypted traffic .....	390
C. Destination reputation analysis.....	390
D. Anomaly of activities on the device after traffic .....	391
Section IV.2.6 Performance of the device .....	392
A. Number of resources needed for data analysis and influence on types of security measures.....	393

---

B. Inter-dependency between applications/components.....	394
Section IV.2.7 Legal provision proposals .....	394
Section IV.2.8 Conclusions .....	397
TITLE V. CONCLUSIONS AND FUTURE WORK.....	400
Chapter V.1 Adjustment of legal requirements to address all entities in the digital ecosystem .....	400
Chapter V.2 Technical limitations and cooperation mechanisms to be implemented at technical and legal levels .....	408
Chapter V.3 Role of each entity in the digital ecosystem and accountability perspective.....	411
Annex 1. Abbreviations.....	416
Annex 2. References.....	417
Annex 3. Questionnaire text .....	471

## *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<sup>1</sup>. 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<sup>2</sup>. 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<sup>3</sup>. 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

---

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> 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.