E-COMMERCE CONSUMER'S PERSONAL DATA PROTECTION

Adriana OTEAN

CZU: 342.4:339.1:004 andreeaotean@gmail.com

The summary of the thesis entitled "E-commerce consumer's personal data protection" focuses on safeguarding the personal data of consumers in the context of distance contracts (hereinafter "e-commerce"). It delves into the legal framework and regulations that govern the protection of personal data in these contractual relationships. By analyzing relevant laws and regulations, the thesis aims to shed light on the specific provisions and requirements aimed at ensuring the privacy and security of consumers' personal information.

The scope of this thesis encompasses a comprehensive examination of the legal and practical aspects surrounding the protection of personal data in e-commerce, as well as, based on what was researched, the proposal of some recommendations both for the legislator and for the e-commerce participants. This thesis explores the rights and/or obligations of both service providers and consumers, the technological solutions available for data protection, and the mechanisms for ensuring data protection. By providing an in-depth analysis of these topics, the thesis aims to offer valuable insights into the complexities of data protection in distance contracting scenarios.

The objectives of this thesis are twofold. Firstly, it aims to critically analyze the existing legal framework and regulations pertaining to the protection of personal data in e-commerce. Through this analysis, the thesis seeks to identify gaps, challenges, and areas for improvement within the current regulatory landscape. Secondly, the thesis aims to propose practical measures and recommendations to enhance the protection of consumers' personal data in e-commerce, thereby contributing to the development of more effective and comprehensive data protection practices.

The legal framework for e-commerce consumer's data protection in the Republic of Moldova and Europe exhibits notable differences. In Europe, the General Data Protection Regulation (GDPR) serves as a comprehensive and harmonized legislation applicable across all EU member states. The GDPR establishes stringent requirements for the processing and protection of personal data, ensuring individuals' rights and placing significant obligations on organizations. In contrast, Moldova has its own set of laws and regulations governing data protection, which may not align entirely with the GDPR. While efforts have been made to harmonize Moldovan legislation with EU standards, there may still be variations in terms of scope, definitions, and enforcement mechanisms. Moldova's legal framework for consumer data protection in e-commerce is shaped by its national laws, such as the Law on Personal Data Protection no.133 dated 8 July 2011, which may not be as comprehensive as the GDPR. It

is important for businesses operating in both regions to be familiar with and adhere to the specific legal requirements in each jurisdiction to ensure compliance and protect consumers' data rights.

Besides the variations in definitions and terminology between the Moldovan law and the GDPR, another important difference lies in the enforcement mechanisms. The GDPR has robust provisions for fines and penalties in case of non-compliance, including significant monetary penalties. In contrast, the Moldovan law on data protection have different penalties and enforcement mechanisms that are specific to the jurisdiction and are not as stringent.

The thesis also explores the risks and challenges associated with protecting consumer's personal data in the context of e-commerce. The chapter begins by identifying the specific risks and challenges that arise in e-commerce concerning the protection of consumers' personal data. It delves into various factors such as data breaches, unauthorized access, and potential vulnerabilities in the e-commerce environment that can compromise the security and privacy of personal data.

Moreover, the chapter evaluates the impact of advanced technologies on the protection of personal data in e-commerce. While technologies such as artificial intelligence, machine learning, and big data analytics offer valuable insights and opportunities for businesses, they also introduce new challenges in terms of data security and privacy. The vast amount of data collected and processed, combined with the complexity of these technologies, increases the potential risks and necessitates robust safeguards.

By addressing these risk factors and challenges comprehensively, stakeholders in e-commerce can develop effective strategies and implement appropriate measures to protect consumers' personal data. It is crucial for businesses to prioritize cybersecurity measures, including regular vulnerability assessments, secure coding practices, and encryption protocols. Additionally, legal and regulatory frameworks should continuously evolve to keep pace with technological advancements, ensuring the enforcement of data protection laws and promoting responsible data practices in e-commerce.

The third chapter of the thesis focuses on the measures employed to ensure the protection of personal data in the context of e-commerce. The chapter examines various measures and technologies aimed at safeguarding consumers' personal data, including encryption, pseudonymization, and privacy-enhancing technologies.

The chapter analyzes different measures, such as encryption and pseudonymization, which are widely used to protect personal data in e-commerce. It also examines the role of privacy policies, informed consent, and data protection officers in ensuring the protection of personal data in e-commerce. Privacy policies provide transparency by informing users about data collection practices, processing purposes, and their rights regarding their personal data.

By considering these measures and technologies, along with the importance of privacy policies, informed consent, and the role of data protection officers, stakeholders in e-commerce can implement a comprehensive approach to data protection. The

effective use of encryption, pseudonymization, and privacy-enhancing technologies helps mitigate risks, while transparent privacy policies and informed consent mechanisms empower individuals to control the use of their personal data. The role of data protection officers ensures accountability and compliance with data protection regulations, fostering a culture of responsible data handling in e-commerce.

In the end, the thesis contains recommendations for aligning the data protection practices in the Republic of Moldova with European provisions and requirements, which include the adoption of comprehensive data protection legislation that mirrors more detailed the principles of the GDPR. Moldova should harmonize its laws with European standards to facilitate data transfers and build trust with European partners. Strengthening data subject rights, such as the right to access, rectify, and erase personal data, is crucial. Implementing robust security measures like encryption and pseudonymization, along with establishing a competent data protection authority, will ensure effective oversight and enforcement.

Also, it is crucial for companies to respect and adhere to the provisions of mandatory security and data protection policies, as these policies play a significant role in safeguarding sensitive information and ensuring the privacy and security of personal data. By implementing mandatory security and data protection policies, companies can establish a framework for effectively managing and protecting personal data collected from customers, employees, and other stakeholders. These policies provide guidelines and best practices for data handling, storage, access control, encryption, and incident response. They help mitigate the risks of data breaches, unauthorized access, and potential misuse of personal information. By implementing these recommendations, Moldova can enhance data protection, foster trust, and align its practices more closely with European data protection standards.

Bibliogrphy:

1. Stewart Room. E-*Commerce Law and Practice in Europe,* p.53-54.
2. Daniel J. Solove, Paul M. Schwartz. *Information Privacy Law*, p.76-79.
3. Hamid Jahankhani, Abbas Bahrampour, Andrew Singh. *Digital Privacy, Data Protection and Online Security: Issues, Challenges, and Solutions,* p.1-2.
4. Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul De Hert. *Data Protection and Privacy*: *The Age of Intelligent Machines,* p.45-51.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council 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), OJ L 119, 4.5.2016, p.1–88.
6. The e-Commerce Directive 2000/31/EC, OJ L 178, 17.7.2000, p.1–16.
7. 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, OJ L 201, 31.7.2002, p.37–47.
8. European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data sub-

jects, adopted on 7 March 2019, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.
9. European Data Protection Board, Guidelines 3/2019 on the processing of personal data through video devices, adopted on 10 January 2019, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.
10. European Data Protection Board, Guidelines 4/2019 on the derogations from Article 49 under Regulation 2016/679, adopted on 12 November 2019, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-derogations-article-49-under-regulation_en.
11. European Data Protection Board, Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR, adopted on 27 November 2019, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en.
12. Directive (EU) 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, OJ L 136, 22.5.2019, p.1–24.
13. Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ L 136, 22.5.2019, p.28–50.
14. Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019, p.7–30.
15. Legea nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal.
16. Constituța Republicii Moldova.
17. Legea nr.982 din 11 mai 2000 privind accesul la informație.
18. Legea nr.142 din 19 iulie 2018 cu privire la schimbul de date și interoperabilitate.
19. European Data Protection Supervisor (EDPS) (2020) Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence.
20. https://advisera.com/articles/list-of-mandatory-documents-required-by-eu-gdpr/
21. https://blogs.sap.com/2022/01/19/challenges-in-cross-border-data-flows-and-data-localization-amidst-new-regulations/
22. Ordinul nr.27 din 31.03.2022 al Centrului Național pentru Protecție a Datelor cu Caracter Personal privind aprobarea Listei tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor cu caracter personal,
23. JØSANG, A. and MARSH, S. The Right of Informational Self-determination and the Value of Privacy: A Legal Perspective. In: *Journal of E-commerce Research and Applications*, vol.5, no.1, p.1-19, Jan.-Feb. 2006.
24. CASTELLUCCIA, C., GASTI, P. and VIGNERI, L. Privacy in E-commerce: Examining User Scenarios and Privacy Preferences. In: *IEEE Security & Privacy*, vol.12, no.1, p.48-55, Jan.-Feb. 2014.
25. BÉLANGER, L. and HILLER, R. *A Framework for E-commerce Privacy.* In: *Communications of the ACM*, vol.42, no.2, p.90-97, Feb. 1999.

26. RENAUD, K. User Perceptions of the Effectiveness of Privacy Enhancing Technologies in E-commerce. In: *Journal of E-commerce Research and Applications*, vol.8, no.3, p.133-142, May-Jun. 2009.
27. PENNEY, J. N. Chilling Effects: Online Surveillance and Wikipedia Use. In: *Berkeley Technology Law Journal*, vol.28, no.1, p.117-182, Jan. 2013.
28. SPIEKERMANN, S. and CRANOR, L. Engineering Privacy. In: *IEEE Transactions on Software Engineering*, vol.30, no.5, p.289-292, May 2004.

Recomandat
***Olesea PLOTNIC**, dr. hab., conf. univ.*