Review of European and Comparative Law

Volume 64 2026/1

e-ISSN 2545-384X

Review of European and Comparative Law

Review of European and Comparative Law

Volume 64 2026/1

Wydawnictwo KUL
Lublin 2026

Proofreading
Paula Ulidowska

Cover design
Paweł Fil

Typesetting
Jarosław Łukasik

The Editor will be pleased to consider contributions provided they are not submitted for publication in other journals. Articles must be presented in their final form in English. Special attention should be given to quotations, footnotes and references, which should be accurate and complete (specific formatting rules are available on the Review website).

The journal is peer-reviewed. A list of reviewers is provided on the journal's website under the link https://czasopisma.kul.pl/index.php/recl/recenzenci.

The journal is co-financed by the Ministry of Education and Science within the programme „Rozw6j czasopism naukowych" [Development of scientific journals]. Contract no. RCN/SN/0287/2021/1 of 14 December 2022.

e-ISSN 2545-384X

The original version is the electronic version.

Wydawnictwo KUL, ul. Konstantynów 1H,
20-708 Lublin, tel. 81 45 45 678
e-mail: wydawnictwo@kul.pl, https://wydawnictwo.kul.pl

TABLE OF CONTENTS

ARTICLES

REVIEW

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 7–24
https://doi.org/10.31743/recl.19392
Received: 19 December 2025 | Accepted: 22 February 2026 | Published: 31 March 2026

Legal Perspectives of Serbia's Healthcare Digitalization: COVID-19 as a Catalyst for Change

Petra Stanojević

Junior Research Assistant, Institute of Social Sciences, Belgrade, Serbia; correspondence address: Kraljice Natalije 45, Belgrade, Republic of Serbia; e-mail: pstanojevic@idn.org.rs
https://orcid.org/0009-0001-0955-2448

Sofija Nikolić Popadić

PhD, Research Associate, Institute of Social Sciences, Belgrade, Serbia; correspondence address: Kraljice Natalije 45, Belgrade, Republic of Serbia; e-mail: snikolic@idn.org.rs
https://orcid.org/0000-0002-5938-4462

Abstract: The COVID-19 pandemic highlighted the critical need for the digitalization of healthcare services worldwide, acting as a catalyst for innovation and prompting governments to reassess healthcare infrastructure and implement legislative and organizational frameworks to support the broader adoption of eHealth solutions. This paper examines Serbia's response during and after the pandemic, addressing whether the experience led to tangible changes in healthcare digitalization. It investigates whether these changes remain largely confined to policy documents and legislation, or if they have been effectively implemented in practice. Furthermore, the study identifies areas where additional improvements are required to ensure that digital healthcare can reach its full potential. Understanding these developments is crucial, not only for preparing for future pandemics but also for responding to other emergencies, improving access to healthcare in remote areas, and supporting vulnerable populations, including older adults. By analyzing Serbia's experience, this paper aims to provide insights into how crises can accelerate digital transformation in healthcare systems and to inform strategies for creating resilient, efficient, and equitable health infrastructures.

Keywords: healthcare digitalization, COVID-19 pandemic, eHealth, telemedicine, health information systems

1. Introduction

The digital transformation of healthcare systems has been an evolving global trend for decades, driven by advances in information and communication technologies, and artificial intelligence (AI)[1] together with the growing need for more efficient, accessible,[2] patient-centered, and data-driven healthcare delivery. The necessity for digitalization of healthcare services was particularly pronounced during the COVID-19 pandemic. At that time, the "need to reduce physical contact has actualized the necessity for application of

[1] Sofija Nikolić Popadić and Marta Sjeničić, "The Use of Artificial Intelligence in Healthcare and Medicine – Legal Aspects," *Journal of Ethics and Legal Technologies* 6, no. 2 (2024): 21–39, https://doi.org/10.14658/pupj-JELT-2024-2-3.

[2] Sofija Nikolić Popadić, "Digitalization of Healthcare Services: The Case of Germany," *Glasnik Advokatske Komore Vojvodine* 92, no. 1 (2020): 89, https://doi.org/10.5937/gakv92-25688.

ISSN 2545-384X (Online)

digital technologies[3] in the process of prevention, diagnosis and treatment of patients" and to widely introduce healing at a distance.[4] Therefore, the pandemic acted as a catalyst for innovation, prompting governments to reevaluate existing healthcare infrastructure and introduce legislative and organizational frameworks to enable the wider implementation of eHealth solutions.

The necessity for change was recognized at both the global and regional levels. International organizations, particularly the World Health Organization (WHO), have emphasized digital health as a cornerstone of sustainable healthcare reform. The WHO's Global Strategy on Digital Health 2020–2025 outlines the importance of integrating digital solutions to "strengthen health systems," improve service access, and enhance resilience in times of crisis.[5] The COVID-19 pandemic also influenced the change at the level of the European Union (EU). Although the EU's role is to "complement national policies" and "encourage cooperation between the Member States," the COVID-19 pandemic showed that there is room for greater EU involvement in healthcare digitalization.[6] The European Health Union was initiated in response to weaknesses identified during the pandemic and to the "need for greater coordination and cooperation in health matters at the EU level."[7] One of the major steps towards digitalization after the pandemic, which is a significant part of the European Health Union, is the European Health Data Space Regulation, adopted in March 2025.[8] All this underscores the growing recognition and importance of further digitalization within the healthcare sector.

The pandemic has impacted the global development of healthcare digitalization.[9] Surveys found that the level of healthcare digitalization before the pandemic, globally and even at the EU level, was unsatisfactory, with some exceptions such as Estonia,

---

3 Giustina Secundo, S.M. Riad Shams, and Francesco Nucci, "Digital Technologies and Collective Intelligence for Healthcare Ecosystem: Optimizing Internet of Things Adoption for Pandemic Management," *Journal of Business Research* 131 (2021): 563–72, https://doi.org/10.1016/j.jbusres.2021.01.034.

4 Sofija Nikolić Popadić, "Introducing Telemedicine – Legal and Other Challenges," in *International Scientific Conference: Challenges and Perspectives of the Development of Legal Systems in the XXI Century – Conference Proceedings* (Banja Luka: Faculty of Law, University of Banja Luka, 2022), accessed November 8, 2025. http://iriss.idn.org.rs/1290/.

5 World Health Organization, "Global Strategy on Digital Health 2020–2025," 2021, accessed November 10, 2025, https://iris.who.int/server/api/core/bitstreams/1f4d4a08-b20d-4c36-9148-a59429ac3477/content.

6 European Court of Auditors, "Digitalisation of Healthcare: EU Support for Member States Effective Overall, but Difficulties in Using EU Funds," Publication Office of the European Union, 2024, accessed November 14, 2025, https://www.eca.europa.eu/ECAPublications/SR-2024-25/SR-2024-25_EN.pdf.

7 Vincent Delhomme and Carina Van Os, "Building the European Health Union (2019–2024): Successes, Limits and Future Perspectives," *European Journal of Risk Regulation* 16, no. 3 (2025): 954, https://doi.org/10.1017/err.2025.10021.

8 Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and Amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L, 2025/327, 5 March 2025).

9 On differences in digitalization efforts in HICs and LMICs, see e.g.: Zisis Kozlakidis, Tracy Wootton, and Karine Sargsyan, "Digital Health: Needs, Trends, Applications," in *Digitalization of Medicine in Low and Middle-Income Countries*, eds. Zisis Kozlakidis, Armen Muradyan, and Karine Sargsyan (Cham: Springer, 2024), 6–7, http://dx.doi.org/10.1007/978-3-031-62332-5; and on the healthcare digitalization level in LMICs in a broader sense: Kozlakidis, Muradyan, Sargsyan, eds., *Digitalization of Medicine in Low and Middle-Income Countries*.

the Netherlands, Denmark and Sweden.[10] The WHO global survey on eHealth found that before the pandemic, only 27% of reporting countries had adopted strategies regarding telemedicine, less than 50% defined medical jurisdiction or liability connected to eHealth services, and less than 30% of countries in the Commonwealth of Independent States and countries of the Central Asian Republics Health Information Network had regulated the use of EHRs.[11] The COVID-19 pandemic primarily impacted healthcare digitalization across 4 areas: communication and information, monitoring and surveillance, healthcare provision, and vaccination.[12] In that sense, globally, during the pandemic and even afterwards, countries have made significant efforts toward healthcare digitalization. Several countries have developed apps to provide essential pandemic information, including Italy, Estonia, Finland, Croatia, the UK, and Canada. Similarly, some countries, such as Bulgaria, Austria, Italy, and the UK, adopted tracking mobile phone movements as a measure to achieve social distancing.[13] The number of remote consultations has heightened globally.[14] Alongside the practical measures, several countries have enacted or amended laws governing the use of eHealth services, particularly e-prescriptions, eSickLeave, and certificates of immunization.[15] In this paper, we will analyze how the COVID-19 pandemic impacted the digitalization of health care services in Serbia. As one of the European countries with the most restrictive lockdown regimes, the need to provide healthcare services through digital systems has become extremely necessary. Namely, besides declaration of state of emergency in the Republic of Serbia (RS), which enabled for derogation from human rights, there was "total ban of movement for citizens over 65 in towns over 5000 inhabitants (and over 70 in smaller towns and villages), nationwide daily curfews for 12 hours including a total ban to leave dwellings during weekends"[16] etc. In such a restrictive situation, with hospitals accepting only emergency cases, providing healthcare services online proved crucial.

We will analyze how Serbia responded during and after the COVID-19 pandemic, aiming to determine whether the pandemic experience has led to changes in the digitalization of healthcare delivery. To compare and identify the extent to which pandemics influenced healthcare, we will first analyze the healthcare situation and level of digitalization before the outbreak of COVID-19. One part of our research will be dedicated to determining whether post-pandemic changes are reflected only in policy documents and legislation, or are actually applied in practice. We will identify the shortcomings, risks,

---

10 Nick Fahy and Gemma A Williams, eds., *Use of Digital Health Tools in Europe: Before, during and after COVID-19* (Copenhagen: World Health Organization, 2021), 7, accessed February 4, 2026, https://www.ncbi.nlm.nih.gov/books/NBK576970/pdf/Bookshelf_NBK576970.pdf.

11 World Health Organization, *Global Diffusion of eHealth: Making Universal Health Coverage Achievable. Report of the Third Global Survey on eHealth* (Geneva: World Health Organization, 2016), 13, 107, 93–99, accessed February 4, 2026, https://iris.who.int/server/api/core/bitstreams/7349d58e-d87b-4330-ab51-82c75ddbfa62/content.

12 Fahy and Williams, eds., *Use of Digital Health Tools in Europe*, 18.

13 Ibid., 19.

14 Ibid., 22.

15 Ibid., 25.

16 Sofija Nikolić Popadić, Marko Milenković, and Marta Sjeničić, "The Covid-19 Epidemic in Serbia – The Challenges of Finding an Appropriate Basis for Responding to a Health Crisis," *Medicine, Law & Society* 14, no. 2 (2021): 234, https://doi.org/10.18690/mls.14.2.229-246.2021.

and challenges of implementing regulations in practice, while highlighting the need for concrete changes, particularly regarding necessary legislation. In the paper, we will determine which improvements and changes remain necessary so that the provision of digital healthcare can fulfil its full potential. This kind of research is important because digital healthcare services would be crucial for potential future pandemics and other emergencies, enabling access to healthcare in remote areas, especially for older generations, etc. By analyzing Serbia's experience, this paper seeks to contribute to a broader understanding of how crises can accelerate digital transformation in healthcare systems and inform future strategies for building resilient, efficient, and equitable health infrastructures.

2. Digitalization of Healthcare Services in Serbia

2.1. Digitalization before the Outbreak of the COVID-19 Pandemic

The need for digitalization of healthcare services in Serbia was acknowledged several decades ago. During the 1990s, the Military Medical Academy in Serbia initiated the development of telemedicine, which at that time encompassed "digitalization and the establishment of telepathological connections between Belgrade and other medical centeres, which brought significant results in medical diagnostics."[17] The foundation of a legislative framework began with the adoption of the Law on Health Care in 2005. It envisages the development of an integrated health information system (HIS), "for the purpose of planning and efficient management of the healthcare system, as well as collection and processing data related to the health condition of the population and the functioning of the health service."[18] The government issued the Regulation on the Program of work, development and organization of the integrated health information system – "e-Health" in 2009, which encompassed the development and management of this system until 2015.[19] The establishment of an integrated HIS and the digitalization of healthcare services in Serbia were and remain long-term processes that require the involvement of various sectors, the provision of appropriate infrastructure at different levels of healthcare, the training of healthcare employees, the digitalization of data, and the inclusion of users. Several projects enabled digitalization and the establishment of the integrated health information system (IHIS) as:

> a central electronic system in which all medical and health data of patients, data of healthcare workers and associates, data of healthcare institutions, health interventions and services performed in healthcare institutions, data of electronic referrals and electronic prescriptions, data on appointments for specialist examinations, diagnostic procedures and surgical interventions are stored and processed.[20]

---

17 Nikola Bošković, "Digital Transformation of the Healthcare System in Serbia: Attitudes of eZdravlje and HIS Users," *BizInfo Blace* 16, no. 1 (2025): 105–13, https://doi.org/10.71159/bizinfo250012B; Branimir Reljin and Vojin Ćućuz, "Projekat Telepatološke Mreže," *XXV Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju PosTel* 2007 (Belgrade), 2007, 101–8.

18 Law on Health Care, Official Gazette of RS, no. 107/2005.

19 Regulation on the Program of Work, Development and Organization of the Integrated Health Information System – 'e-Health,' Official Gazette of RS, no. 95/2009.

20 Ministry of Health, "Integrated Health Information System of the Republic of Serbia."

To fully establish and implement it, it was necessary to amend existing laws and enact new ones. The Law on health documentation and records in the field of health, which entered into force in 2014 and has been in effect since January 1, 2017, served as a more detailed foundation for establishing IHIS and the digitalization of health care services.[21] It regulates health documentation and records that serve as the basis for the functioning of the IHIS, especially the part related to maintaining documentation in electronic form. Data from the patient's medical records were recognized as particularly sensitive personal data, which should be handled in accordance with the law governing the protection of personal data[22] – at that time, the Personal Data Protection Law from 2009. Unfortunately, that law recognized only the particular sensitivity of health data and lacked detailed regulation. In 2018, the Law on Personal Data Protection[23] was adopted, which is largely harmonized with the EU General Data Protection Regulation (GDPR). The right to the confidentiality of data on the patient's state of health and the recognition of health data as sensitive personal data were prescribed in that law and in the Law on Patients' Rights,[24] both of which are very significant for the digitalization of healthcare. Since 2019, the organization and development of IHIS have also been partly regulated by the Law on Health Care.[25] From our analysis, we can conclude that the digitalization of the healthcare sector before the COVID-19 pandemic was still developing, despite the establishment of IHIS. It had weaknesses and implementation inconsistencies, particularly in data protection.

Before the outbreak of the COVID-19 pandemic, certain digital services were available. Since 2015, it has been possible to schedule an appointment with a general practitioner via the My Doctor application; electronic prescriptions were gradually introduced, culminating in full implementation in 2019; and since 2017, it has been possible to check health insurance status via the website of the Republic Health Insurance Institute. But the pandemic has shown that the level of digitalization, especially in the provision of health services, was not satisfactory and that there is a need for change to ensure its availability in the context of a pandemic, when physical contact and the possibility of coming to the clinic were limited.

2.2. Changes in the Digitalization of Healthcare during the COVID-19 Pandemic

Some specific digital services were introduced during the pandemic to reduce physical contact. One of them is the electronic vaccination system (e-vaccine). The first step in this system was online registration for vaccination via e-administration or by phone. After that, citizens received information via email and SMS about when and where to come for vaccination. This system enabled tracking of the serial number of each dose and recording

21 Law on Health Documentation and Records in the Field of Health, Official Gazette of RS, no. 123/2014.
22 Ibid., Articles 40, 50.
23 Law on Personal Data Protection, Official Gazette of RS, no. 87/2018.
24 Law on Patients' Rights, Official Gazette of RS, no. 45/2013, 25/2019, Articles 21, 22.
25 Unfortunately, only one article was dedicated specifically to IHIS. Law on Health Care, Official Gazette of RS, no. 25/2019.

of each citizen who received the vaccine.[26] The Digital Green Certificate, introduced during the pandemic, served as a confirmation of COVID-19 vaccination, including test results for infection and recovery, and was compatible with the EU certificate.[27]

The need to provide health services to non-COVID-19 patients was pronounced, raising questions about the feasibility of introducing telemedicine (healing at a distance). The lack of legal regulation represented a significant obstacle to the wider implementation of telemedicine at that time, when it was most needed. There were some attempts to introduce e-consultations, especially for psychological support during the pandemic. A free national helpline, called "How are you doing?," was established after the outbreak of COVID-19 to provide psychosocial support by telephone.[28] Since May 2021, there has been a "unified free service for mental healthcare of the Ministry of Health of the RS and the Clinic for Mental Disorders Dr Laza Lazarević," available via phone 24 hours a day.[29] Through that helpline, there were more than 30.000 interventions during the pandemic, in the form of "support, counselling, short psychotherapy (crisis) interventions, as well as recommendations related to already prescribed medication," given by "qualified health workers and consultants of the Clinic."[30] This showed how important telephone consultations are during a crisis.

The pandemic has shown that it is necessary to accelerate the digitalization of healthcare and enable wider application of digital services in practice. The need for the implementation of healing at a distance in conditions of reduced movement and contact has been particularly pronounced, underscoring the necessity of enabling the application of telemedicine on a wider scale, not just within pilot projects as was the case before the COVID-19 pandemic.[31] But broader digitalization required amending existing regulations and adopting new ones. In the next section, we will dedicate our research to answering whether this has been done after the pandemic and to the current status of healthcare digitalization in Serbia.

2.3. Digitalization Efforts after the COVID-19 Pandemic

Serbia emerged from the pandemic with several e-services introduced in the healthcare sector. Among the most important services currently available to citizens are ePrescription,[32] eRadiology, eInvoice, eReferral (with referral validation for surgery still pending),

---

26 Government of the Republic of Serbia, "New E-Vaccine System for Monitoring Immunization," 2021, accessed December 9, 2025, www.srbija.gov.rs/vest/512847/pokrenut-novi-sistem-e-vakcina-za-pracenje-imunizacije.php.

27 E-administration, "EU Digital Green Certificate," 2021, accessed November 29, 2025, https://euprava.gov.rs/usluge/6962.

28 Nikolić Popadić, "Introducing Telemedicine – Legal and Other Challenges," 350. Ivana Stašević-Karličić, "How Much Has the COVID-19 Pandemic Changed Us: The Experience of the Clinic for Mental Disorders 'Dr Laza Lazarević'," *Srpski Medicinski Casopis Lekarske Komore* 2, no. 3 (2021): 295–301, https://doi.org/10.5937/smclk2-33326.

29 Ibid.

30 Ibid.

31 See: Nikolić Popadić, "Introducing Telemedicine – Legal and Other Challenges," 349.

32 Government of the Republic of Serbia, "ePrescription: The Future Is Now," accessed December 3, 2025, https://www.srbija.gov.rs/tekst/329843/erecept.php.

and the Electronic Health Record (which is not yet fully standardized).[33] Several services are still in the pipeline, with full implementation planned in the near future, such as eSickLeave.[34]

The most notable progress has been achieved in strengthening the legal framework governing both existing and planned digital services, as well as in establishing a Coordination Body for the Digitalization of the Healthcare System in 2021.[35] The Programme of Digitalization in the Healthcare System of the Republic of Serbia for the Period 2022–2026 was adopted in February 2022. The general objective is defined as "the digitalization of the healthcare system and the safe use of digital services and technologies to ensure higher-quality, more efficient, and more accessible healthcare."[36] A key measure identified to achieve this goal is the establishment of a unified Electronic Health Record (EHR). Furthermore, the Programme outlines the IHIS, which comprises both central and local information systems. The central system is designed to facilitate collaboration among all stakeholders in healthcare provision, ensuring data sharing and authorized access. The local systems implemented in public and private healthcare institutions are used to record and track patient medical data and to support day-to-day operations and institutional functions.[37] The Programme recognized the importance of telemedicine, through measure 2.7 (Establishment of electronic services for users of health services) and adoption of the "Telemedicine implementation plan in the health care system" as one of the planned activities.

The corresponding Action Plan for the Period 2022–2023 identified activities necessary for the successful implementation of the Programme.[38] The most important measures included: aligning the legal framework with the Law on Electronic Government; establishing a legal framework for the development and maintenance of a unified IHIS architecture; creating an organizational unit within the Ministry of Health to manage healthcare digitalization and supporting organizational unit within the Office for Information Technology and E-Government; improving the legal framework for maintaining medical documentation and records in electronic form. The Government has prepared the new 2024–2025 Action Plan, intended to build on numerous international programs

33 "European Health Data Space: Serbia's Path Forward," EIT Health, Serbia Center for the Fourth Industrial Revolution, 2025, 10, accessed December 10, 2025, https://c4ir.rs/wp-content/uploads/2025/11/EHDS-Serbia-White-Paper-Report_FINAL.pdf.

34 Ministry of Health – eHealth Portal, "eSickLeave: Data and Documentation from the Central System," February 6, 2025, accessed November 29, 2025, https://e-zdravlje.gov.rs/news/ebolovanje-podaci-i-dokumentacija-iz-centralnog-sistema-ebolovanje-4; EIT Health, "European Health Data Space," 10; during the preparation of this paper, the Parliament of Serbia adopted the Law on the Exchange of Data, Documents and Information in Cases of Temporary Incapacity for Work Using the Software Solution "eSickLeave – Employer," whose implementation is planned for January 2026.

35 Government of the Republic of Serbia, "Formira se Koordinaciono telo za digitalizaciju u zdravstvenom sistemu," 2021, accessed November 26, 2025, https://www.srbija.gov.rs/vest/512076/formira-se-koordinaciono-telo-za-digitalizaciju-u-zdravstvenom-sistemu.php.

36 Government of the Republic of Serbia, "The Digitalization Programme for the Serbian Health Care for the Period 2022–2026," 2022, 16, accessed December 3, 2025, https://www.zdravlje.gov.rs/tekst/364590/program-digitalizacije-u-zdravstvenom-sistemu.php.

37 Ibid., 18.

38 Ibid.

and continue the activities initiated under the previous plan. Still, our research shows it is not (yet) publicly available.[39]

Most of the measures from the Action Plan have not yet been achieved. Our research results show that none of the legal acts intended to be harmonized with the Law on Electronic Government – the Law on Healthcare, Law on Health Insurance, Law on Medicinal Products and Medical Devices, and Law on Patients' Rights – have been amended in accordance with the Action Plan. Exceptionally, measures focused on establishing the legal framework for the IHIS architecture and maintaining medical documentation and records in electronic form were accomplished through the enactment of the Law on Health Documentation and Health Records (LHDHR) in October 2023.

The LHDHR introduces the electronic health record (EHR), defining it as a "unified and centralized register comprising data and documents from mandatory medical documentation maintained in electronic form, exercising rights arising from compulsory health insurance, for analytics, reporting, health system planning and scientific research purposes."[40] The law obliges the Ministry of Health to establish and maintain necessary registers (primarily the EHR), e-services, and software solutions,[41] as well as the IHIS, with technical support from the Office for Information Technology and Electronic Government. It contains provisions regarding data security and safety, explicitly stating that the information contained in a patient's medical documentation constitutes a special category of personal data.

To support its effective implementation, several bylaws and supplementary acts have been introduced. Most notably, the Rulebook on the e-Record, the Personal Health Number and the Delivery of Data upon a Patient's Personal Request[42] is scheduled to come into effect on January 1, 2026. The Rulebook specifies that the EHR is established by retrieving data from the software solutions used by healthcare institutions, private practices, and other legal entities, or from registers managed by the Ministry for Health.[43] It further regulates the content of data, the procedures for their collection, and the conditions under which authorized personnel can access them.

Initial steps towards establishing a legal framework for the use of AI have been taken with the adoption of the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the Period 2025–2030. The Strategy explicitly identifies incentives for the application of AI in healthcare as one of the envisaged measures.[44] However, it does not include specific provisions on the use of AI in healthcare, and the law that would comprehensively regulate this issue still does not exist.

---

39 Government of the Republic of Serbia, "Action Plan for the Period 2024–2025 for the Implementation of the Digitalization Program in the Healthcare System of the Republic of Serbia for the Period 2022–2026," accessed December 13, 2025, https://ekonsultacije.gov.rs/topicOfDiscussionPage/308/1.

40 The Law on Health Documentation and Health Records, Official Gazette of RS, no. 92/2023, 2023, Article 4, para. 1, item 7.

41 The Law on Health Documentation and Health Records, Article 34, para. 1.

42 The Rulebook on the E-Record, the Personal Health Number and the Delivery of Data upon a Patient's Personal Request, Official Gazette of the Republic of Serbia, No. 45/2025, 2025.

43 Ibid., Article 2, para. 1.

44 Government of the Republic of Serbia, Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the Period 2025–2030, Official Gazette of the RS, No. 5/ 2025, 2025, measure 6.7.

Finally, the Law on the Exchange of Data, Documents and Information in Cases of Temporary Incapacity for Work Using the Software Solution "eSickLeave – Employer" was enacted in December 2025, with general purpose of "establishment of a timely, reliable and binding system of electronic exchange of data, documents and notifications in the procedure for exercising the right to salary compensation based on temporary incapacity for work."[45] This is primarily achieved through the introduction of mandatory use of the "eSickLeave – Employer" software solution.

Although significant efforts have been made to harmonize the legal framework for healthcare digitalization, gaps remain. The framework is inconsistent, and conflicts between provisions of different laws are common. It is therefore important to continue aligning regulations listed in this section (primarily harmonizing laws listed in the Action Plan with the Law on Electronic Government) to address the problem of essentially identical processes being regulated differently.[46]

3. Analysis of Implementation of eHealth Services in Practice

Even though Serbia has come a long way in digitalizing its healthcare,[47] with several e-services being available to citizens, there is still hesitance in their practical application. This segment of the paper will examine whether the provided services are being adequately implemented in practice and analyze citizens' attitudes toward them.

The State Audit Institution of Serbia has highlighted several areas in which the country is falling short of its envisioned goals in this process (stable financing, IT risk management, the lack of educational programs, privacy risks associated with the non-uniformity of user registration, etc.).[48] Concerning privacy risks, it stressed the inadequacy of relationships with service providers concerning data protection. Although most contracts include confidentiality clauses, there is no mechanism to ensure compliance, which may lead to the disclosure of sensitive health data.[49] Privacy risks arise from the collection, storage, and transfer of intimate patient data.[50] Patients in Serbia are often unaware of how the processed data is protected,[51] which increases their distrust in the system. Similarly, medical professionals have expressed concerns about systems'

45 The Law on the Exchange of Data, Documents and Information in Cases of Temporary Incapacity for Work Using the Software Solution "eSickLeave – Employer," Official Gazette of the Republic of Serbia, No. 109/2025, 2025, Article 1.

46 European Commission, Interoperable Europe Portal, "Serbia Digital Public Administration Factsheet Supporting Document," 2024, 4, accessed November 25, 2025, https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/digital-public-administration-factsheets-2024.

47 Some surveys indicate that the overall performance of the IHIS improved by 0.9 points from 2021 to 2024. See: Bosiljka Djikanovic et al., "Serbian Health Information System (HIS) Improvements 2021–2024: Comparison Study Using Stages of Continuous Improvement (SOCI) Methodology," *Health Research Policy and Systems* 23, no. 1 (2025): 8, https://doi.org/10.1186/s12961-025-01337-5.

48 State Audit Institution of the Republic of Serbia, "Performance Audit Report – Information Security in Healthcare Information Systems," 2021, accessed November 25, 2025, https://www.dri.rs/izvestaj/3410.

49 Ibid., 9.

50 Nicholas Cummins and Björn Schuller, "Five Crucial Challenges in Digital Health," *Frontiers in Digital Health* 2 (2020): 2, https://doi.org/10.3389/fdgth.2020.536203.

51 Cummins and Schuller, "Five Crucial Challenges in Digital Health," 2.

vulnerability to cyberattacks.[52] Recognized risks are highlighted by the lack of consent withdrawal in the eHealth portal[53] and by the software's ability to permanently store data even after deletion.[54]

The EHR does not provide all necessary data, either due to system errors or because physicians fail to fulfil their obligations. Reports from specialists regarding examinations conducted on referrals are often not visible, which contributes to the system's inefficiency.[55]

The system's shortcomings often stem from outdated hardware and software. More than half of users report occasional system downtime, while a significant percentage find the system interface unintuitive.[56] The existing infrastructure in rural facilities, combined with unstable internet connectivity, compromises the provision of healthcare services.[57]

One obstacle to the broader use of the eHealth application is the complex registration process.[58] Many citizens do not have an eGovernment account, which is created in person for authorization and authentication, and electronic registration from home is not possible. Moreover, a large percentage of the population does not have an electronic certificate and is unable to use eHealth services.

Results from surveys aiming to assess the level of users' familiarity with eHealth services and the extent to which they utilize them[59] show that a large percentage of the population has expressed distrust and reluctance toward the digitalization process, with a significant number not well informed about the available services (in some surveys, 4/5 of respondents are unfamiliar with eHealth applications).[60] Only a small part of the population uses the application regularly, with only 8.4% of respondents scheduling appointments electronically, and nearly a third still scheduling by phone calls.[61] More than half of the respondents do not use an eHealth application at all.[62] Healthcare providers typically hold a more positive view; however, a significantly high percentage is dissatisfied with the system's functionality.[63] All of this highlights the need for broader

52 Marko Milić, "Critical Assessment of the HELIANT System in Healthcare in Serbia: Opportunities, Challenges, and Future Directions," Zenodo, December 29, 2024, 17, https://doi.org/10.5281/zenodo.14569252.

53 EIT Health, "European Health Data Space," 14.

54 Branko Marović et al., "E-Hospital, Children's University Hospital in Belgrade and HELIANT Hospital Information System," *MD Medical Data* 1, no. 4 (2009): 77.

55 NALED, *Grey Book of Healthcare* (Belgrade: NALED, 2020), 12, accessed November 26, 2025, https://naled.rs/htdocs/Files/04612/Siva_knjiga_zdravstva.pdf.

56 Milić, "Critical Assessment of the HELIANT System," 14.

57 Ibid., 16.

58 See more: Ministry of Health, "User Guide – eHealth Patient Portal," accessed December 9, 2025, https://e-zdravlje.gov.rs/landing/repository/documents/user-manual-sr.pdf.

59 Ilija Gavrilović, "Izazovi u Korišćenju Portala E-Uprava i Elektronskih Usluga u Srbiji," *Politička Revija* 85, no. 3 (2025): 70, https://doi.org/10.5937/pr85-60522. See similarly for EU-members: Andrea Floria, Ștefan Burcea, and Corina Folescu, *Challenges Encountered in the Use of Electronic Services in the Public Administration from EU Member States* (Romania: ACZ Consulting, 2019), https://www.eupan.eu/wp-content/uploads/2019/06/RO-EUPAN-Comparative-Study-Public-Electronic-Services.pdf.

60 Bošković, "Digital Transformation of the Healthcare System in Serbia," 7.

61 Ibid., 6.

62 Ibid., 5.

63 Ibid., 7.

promotion of developed services and for the involvement of NGOs, patient organizations, and healthcare workers in the decision-making and implementation processes.

The extent to which users use the services depends on the level of internet access and digital literacy. Ensuring equal access to healthcare is of utmost significance, particularly in light of the primary objectives established in legislation. Serbia should prioritize ensuring equal access to the internet, increasingly recognized as a human rights issue and a prerequisite for accessing healthcare services. According to data from the Statistical Office of the RS for 2025, 90.1% of households in Serbia had internet access.[64] However, the results of the 2022 Census showed that only about 46% of the population aged 15 and over can be considered computer-literate (able to perform three basic computer-related activities). Around 30% of the population is partially literate, while 24% is considered computer illiterate.[65] Disparities in digital literacy can impede patients' ability to navigate digital health portals or assess the reliability of telemedical advice, placing certain groups at a heightened risk of misunderstanding or misuse.[66]

This aligns with similar surveys conducted worldwide, particularly those focused on low- and middle-income countries (LMICs). One study on mobile internet use in LMICs found that 3.4 billion people globally are not using mobile internet, with key barriers including a lack of resources to afford an internet-enabled phone, a lack of (digital) literacy, and security concerns.[67] On the other side, among those who use mobile internet, only a small percentage use it for health services. The survey found that in most LMICs, the percentage of people who have (even once) accessed eHealth services is concerning low, with only 16% in Pakistan, 23% in Senegal, 29% in Ethiopia, and 30% in Indonesia.[68] The survey found that eHealth services are among the services users are least aware of.[69] This only shows that the unsatisfactory level of eHealth service use, as well as the level of digital literacy as one of its factors, is not a problem confined to Serbia but is connected to broader issues in LMICs. When comparing this data to the EU, we

64 Internet availability was highest in the Belgrade region, at 95.5%. In the Vojvodina region, it amounted to 88.8%, in the Šumadija and Western Serbia region 88.3%, and in the Southern and Eastern Serbia region 86.7%; Statistical Office of the Republic of Serbia, "Use of ICT – Households, 2025," 2025, accessed December 13, 2025, https://www.stat.gov.rs/sr-latn/vesti/20251024-upotreba-ikt-a-domacinstva-2025/?s=2701.

65 Statistical Office of the Republic of Serbia, "The 2022 Census of Population, Households and Dwellings: Educational Attainment, Literacy and Computer Literacy," 2023, accessed December 13, 2025, https://publikacije.stat.gov.rs/G2023/Pdf/G20234006.pdf.

66 Motti Haimi, "The Tragic Paradoxical Effect of Telemedicine on Healthcare Disparities- a Time for Redemption: A Narrative Review," *BMC Medical Informatics and Decision Making* 23, no. 1 (2023): 95, https://doi.org/10.1186/s12911-023-02194-4.

67 Matthew Shanahan and Kalvin Bahia, "The State of Mobile Internet Connectivity 2025: Barriers to Mobile Internet Adoption and Use," GSMA Intelligence, 2025, 6, accessed February 4, 2026, https://www.gsma.com/somic/wp-content/uploads/2025/11/The-State-of-Mobile-Internet-Connectivity-2025-Barriers-to-Mobile-Internet-Adoption-and-Use.pdf

68 Matthew Shanahan and Kalvin Bahia, "The State of Mobile Internet Connectivity 2025: Understanding Mobile Internet Use in Low- and Middle-Income Countries," GSMA Intelligence, 2025, 38, accessed February 4, 2026, https://www.gsma.com/somic/wp-content/uploads/2025/09/The-State-of-Mobile-Internet-Connectivity-2025-Understanding-Mobile-Internet-Use-in-LMICs.pdf.

69 Ibid., 13.

found that the difference in digital literacy levels, even though not drastic, still exists. In 2023, 56% of people aged 16–74 in the EU had (at least) basic digital skills, with some countries exceeding 80%, such as the Netherlands (83%) and Finland (82%). However, some EU countries have shown a higher level of digital illiteracy than Serbia, such as Romania (28%) and Bulgaria (36%).[70] Similarly, reports have highlighted the uneven use of eHealth services on the EU level, despite their overall "widespread availability," with 73% of the population accessing their EHR in Finland to only 5% in Germany in 2024. The average EHR use across the EU in 2024 was only 28%.[71]

In conclusion, the level of digital literacy as a prerequisite for broader use of eHealth services, albeit on a larger scale in LMICs, still poses a significant barrier to the accessibility and effectiveness of healthcare provision globally.

4. Discussion

Our research results identify several obstacles and challenges that still need to be overcome. As is the case for most developing countries,[72] Serbia is experiencing a lack of available resources necessary for digitalization; the used hardware and software are often outdated;[73] the technological infrastructure is uneven;[74] and there is a shortage of qualified IT personnel. Investing in adapting hardware and software solutions is a key step toward enhancing service quality.

There is a lack of alignment across health sectors, which poses a barrier to creating a unified EHR. Serbia's healthcare is divided into three sectors – public, private, and military - which operate independently with little to no cooperation. Difficulties arising from the decentralization of collected data include the inability of medical professionals to access all patient information, duplicate medical visits, and generally inefficient healthcare provision.[75] The private sector is not adequately integrated into the digitalization process; the EHR does not include data on services provided in the private sector;[76] and electronic appointment scheduling in private institutions is not available through the My Doctor application.[77]

---

70 Eurostat, "Skills for the Digital Age," April 2024, accessed February 4, 2026, https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=628712.

71 OECD, "Synthesis Report 2025: Health Policy Reform Trends in the EU," 2025, 21, accessed February 4, 2026, https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/synthesis-report-2025-health-policy-reform-trends-in-the-eu_f661ffc5/1f6a8e9a-en.pdf.

72 Berislav Vekić et al., "Implementation of the Nationwide Electronic Health Record System in Serbia: Challenges, Lessons Learned, and Early Outcomes," *Acta Clinica Croatia* 61, no. 3 (2022): 489, https://doi.org/10.20471/acc.2022.61.03.14.

73 Petar Rajković et al., "The Role of Resource Awareness in Medical Information System Life Cycle," *Arxiv*, (2022): 2, https://arxiv.org/abs/2205.07778.

74 Milić, "Critical Assessment of the HELIANT System," 3.

75 EIT Health, "European Health Data Space," 10.

76 Jelena Bojović, and Milica Stefanović, eds., "Grey Book 16 – Recommendations for Removing Administrative Obstacles to Doing Business in Serbia 2024," NALED, 2024, 44, accessed December 3, 2025, https://naled.rs/htdocs/Files/14377/Siva-knjiga-SRB.pdf.

77 Bošković, "Digital Transformation of the Healthcare System in Serbia," 7.

Our results show a need to unify the data across sectors and integrate the private healthcare system with the public one. This would involve enabling medical professionals employed in private healthcare institutions to access patient data from the public sector, and vice versa. The steps towards achieving this unification have been taken through the enactment of the LHDHR, which established the EHR, but its full implementation is still pending.[78]

The research results and data presented in the previous section show that the level of digital literacy remains a crucial obstacle that Serbia must overcome. A large part of Serbia's population is elderly people with little to no technological skills, raising questions about healthcare accessibility[79] and availability. The lack of technical training for medical professionals reduces the system's efficiency, leading to an undesirably high number of doctors opting for physical rather than electronic record-keeping. This issue translates into healthcare providers' inability to implement digital solutions and fully understand digital tools in use.[80] Furthermore, due to employment prohibitions, the positions designated for IT specialists are often filled by individuals of other professional backgrounds.[81] Accordingly, emphasis should be placed on providing healthcare workers and the general public with technological education through courses and continuous programs. Furthermore, users' distrust can be solved by involving NGOs, patient organizations, and healthcare workers in the decision-making process.

When discussing privacy risks connected to digitalization, it is important to acknowledge that Serbia has an established legal framework for the protection of personal data. The Law on Personal Data Protection is largely harmonized with the GDPR. Significant efforts are made to mitigate risks through the authentication process for signing up for e-services. Authentication, enabled by the ConsentID application, uses qualified electronic certificates.[82] However, IHIS audits continue to identify information security issues related to service providers' access to the database.[83]

Going forward, a priority should be the development of several envisioned, yet still unrealized services – primarily eSicknessLeave and eReferral, which are still not fully operational in enabling the validation of referrals for surgery.[84] Proposals have been made to implement AI chatbots[85] that would allow citizens to acquire basic medical information in real time. Such tools could increase the accessibility of healthcare but pose a number of serious risks, including patient harm due to AI errors, misuse, bias, and

78 NALED, "Report on Activities and Implementation of NALED's Strategic Goals for 2023 and Overview up to 2025," 2024, 29, https://naled.rs/htdocs/Files/14953/Report-on-Strategic-goals-realization-2023-24.pdf. Similarly see: NALED, "Annual Report on the Activities and Implementation of NALED's Strategic Goals 2024/25," 2025, https://naled.rs/htdocs/Files/17551/Report-on-Strategic-goals-realization-2024-25.pdf.

79 Government of the Republic of Serbia, "Digitalization Programme," 15.

80 EIT Health, "European Health Data Space," 15.

81 Government of the Republic of Serbia, "Digitalization Programme," 13.

82 Marija Zajeganović et al., "Data Security in Mobile Healthcare," *Military Technical Courier* 71, no. 3 (2023): 763, https://doi.org/10.5937/vojtehg71-44245.

83 State Audit Institution of the Republic of Serbia, "Performance Audit Report," 2.

84 EIT Health, "European Health Data Space," 10.

85 Aldina Avdić, "Realizacija Servisa Pametnog Zdravstva i Njihova Integracija u Koncept Pametnih Gradova," (PhD diss., University of Niš, 2021), 73–74, https://nardus.mpn.gov.rs/handle/123456789/20732.

gaps in accountability.[86] The increasing use of AI-driven diagnostic and decision-support systems may also limit patients' understanding of how clinical judgments are formed, thereby complicating informed consent and potentially undermining trust in the physician-patient relationship.[87] Serbia still has not adopted a law that would regulate the use of AI in detail, and this should be one of the first steps to avoid the realization of previously identified risks.

Regarding legislative efforts, there is a need to harmonize the framework by adopting by-laws established under the LHDHR, as well as the Law on Healthcare and Health Insurance for Military Insured Persons. As previously discussed, none of the laws envisioned to be harmonized with the LHDHR has been amended. Similarly, telemedicine, although its significance was pronounced during the COVID-19 pandemic and later recognized in the Digitalization Programme, remains unregulated, and there are still no draft laws governing it.[88]

The effective implementation of envisioned measures requires the establishment of specialized bodies to oversee their execution. It is necessary to establish a coordination body for digitalization within the healthcare system, alongside a dedicated organizational unit within the Office for IT and eGovernment.[89]

5. Conclusion

The research results highlight the importance of healthcare digitalization not only during crises but also as a means to make healthcare services more accessible, especially in rural areas. In conclusion, it is important to emphasize that Serbia has made considerable improvements in this process following the COVID-19 pandemic. The number of available e-services has substantially increased, notable legislative efforts have been undertaken, and new specialized bodies have been established. Serbia has recognized the importance of digitalization and envisioned it as one of the key objectives to pursue. However, as previously discussed, several challenges continue to hinder invested efforts. Some of these challenges are related to the digitalization process itself and are common to most countries (primarily privacy risks). In contrast, others are specific to Serbia (sectoral fragmentation, digital illiteracy, resource availability, etc.). This paper contributes to the literature by exploring how the pandemic accelerated Serbia's digitalization process and its current status. We analyzed the practical implementation of adopted solutions and users' familiarity with them, concluding that it is not yet satisfactory due to multiple factors. Finally, we provided several recommendations for the future development of healthcare digitalization and proposed actions necessary to overcome the identified obstacles. We hope that this paper will further the discussion recently opened in the literature and serve as a useful guide for policymakers and other stakeholders in their future decisions,

86 Nikolić Popadić and Sjeničić, "The Use of Artificial Intelligence in Healthcare and Medicine," 24 and more.
87 Ibid., 25–26.
88 More on the importance and benefits of telemedicine and its regulation, see: Nikolić-Popadić, "Introducing Telemedicine – Legal And Other Challenges," 348 and more.
89 EIT Health, "European Health Data Space," 16–17.

as it identifies challenges and obstacles, highlights legislation that needs to be mutually harmonized, and proposes solutions for the successful implementation of healthcare digitalization.

Funding: This paper was written as part of the 2025 Research Program of the Institute of Social Sciences supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia.

References

Avdić, Aldina. "Realizacija Servisa Pametnog Zdravstva i Njihova Integracija u Koncept Pametnih Gradova." PhD diss., University of Niš, 2021. https://nardus.mpn.gov.rs/handle/123456789/20732.

Bojović, Jelena, Milica Stefanović, eds. "Grey Book 16 – Recommendations for Removing Administrative Obstacles to Doing Business in Serbia 2024." NALED, 2024. Accessed December 3, 2025. https://naled.rs/htdocs/Files/14377/Siva-knjiga-SRB.pdf.

Bošković, Nikola. "Digital Transformation of the Healthcare System in Serbia: Attitudes of eZdravlje and HIS Users." *BizInfo Blace* 16, no. 1 (2025): 105–13. https://doi.org/10.71159/bizinfo250012B.

Cummins, Nicholas, and Björn Schuller. "Five Crucial Challenges in Digital Health." *Frontiers in Digital Health* 2 (2020): 1–5. https://doi.org/10.3389/fdgth.2020.536203.

Delhomme, Vincent, and Carina van Os. "Building the European Health Union (2019–2024): Successes, Limits and Future Perspectives." *European Journal of Risk Regulation* 16, no. 3 (2025): 942–60. https://doi.org/10.1017/err.2025.10021.

Djikanovic, Bosiljka, Milan Kovacevic, Isidora Smigic, Marija Cvejic, Emilija Nicic, Caitlin Madevu-Matson, Steve Ollis et al. "Serbian Health Information System (HIS) Improvements 2021–2024: Comparison Study Using Stages of Continuous Improvement (SOCI) Methodology." *Health Research Policy and Systems* 23, no. 1 (2025): 92. https://doi.org/10.1186/s12961-025-01337-5.

E-administration. "EU Digital Green Certificate," 2021. Accessed November 29, 2025. https://euprava.gov.rs/usluge/6962.

EIT Health, Serbia Center for the Fourth Industrial Revolution. "European Health Data Space: Serbia's Path Forward," 2025. Accessed December 10, 2025. https://c4ir.rs/wp-content/uploads/2025/11/EHDS-Serbia-White-Paper-Report_FINAL.pdf.

European Commission, Interoperable Europe Portal. "Serbia Digital Public Administration Factsheet Supporting Document," 2024. Accessed November 25, 2025. https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/digital-public-administration-factsheets-2024.

European Court of Auditors. "Digitalisation of Healthcare: EU Support for Member States Effective Overall, but Difficulties in Using EU Funds." Publication Office of the European Union, 2024. Accessed November 14, 2025. https://www.eca.europa.eu/ECAPublications/SR-2024-25/SR-2024-25_EN.pdf.

Eurostat. "Skills for the Digital Age," April 2024. Accessed February 4, 2026. https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=628712.

Fahy, Nick, and Gemma A. Williams, eds. *Use of Digital Health Tools in Europe: Before, during and after COVID-19*. Copenhagen: World Health Organization, 2021. Accessed February 4, 2026. https://www.ncbi.nlm.nih.gov/books/NBK576970/pdf/Bookshelf_NBK576970.pdf.

Floria, Andrea, Ștefan Burcea, and Corina Folescu. *Challenges Encountered in the Use of Electronic Services in the Public Administration from EU Member States*. Romania: ACZ Consulting, 2019.

https://www.eupan.eu/wp-content/uploads/2019/06/RO-EUPAN-Comparative-Study-Public-Electronic-Services.pdf.

Gavrilović, Ilija. "Izazovi u Korišćenju Portala E-Uprava i Elektronskih Usluga u Srbiji." *Politička Revija* 85, no. 3 (2025): 63–86. https://aseestant.ceon.rs/index.php/polrev/article/view/60522.

Government of the Republic of Serbia. "Action Plan for the Period 2024–2025 for the Implementation of the Digitalization Program in the Healthcare System of the Republic of Serbia for the Period 2022–2026." Accessed December 13, 2025. https://ekonsultacije.gov.rs/topicOfDiscussionPage/308/1.

Government of the Republic of Serbia. "ePrescription: The Future Is Now." Accessed December 3, 2025. https://www.srbija.gov.rs/tekst/329843/erecept.php.

Government of the Republic of Serbia. "Formira se Koordinaciono telo za digitalizaciju u zdravstvenom sistemu," 2021. Accessed November 26, 2025. https://www.srbija.gov.rs/vest/512076/formira-se-koordinaciono-telo-za-digitalizaciju-u-zdravstvenom-sistemu.php.

Government of the Republic of Serbia. "New E-Vaccine System for Monitoring Immunization," 2021. Accessed December 9, 2025. https://www.srbija.gov.rs/vest/512847/pokrenut-novi-sistem-e-vakcina-za-pracenje-imunizacije.php.

Government of the Republic of Serbia. "The Digitalization Programme for the Serbian Health Care for the Period 2022–2026," 2022. Accessed December 3, 2025. https://www.zdravlje.gov.rs/tekst/364590/program-digitalizacije-u-zdravstvenom-sistemu.php.

Haimi, Motti. "The Tragic Paradoxical Effect of Telemedicine on Healthcare Disparities- a Time for Redemption: A Narrative Review." *BMC Medical Informatics and Decision Making* 23, no. 1 (2023): 95. https://doi.org/10.1186/s12911-023-02194-4.

Kozlakidis, Zisis, Armen Muradyan, and Karine Sargsyan, eds. *Digitalization of Medicine in Low and Middle-Income Countries*. Cham: Springer, 2024. http://dx.doi.org/10.1007/978-3-031-62332-5.

Kozlakidis, Zisis, Tracy Wootton, and Karine Sargsyan. "Digital Health: Needs, Trends, Applications." In *Digitalization of Medicine in Low and Middle-Income Countries*, edited by Zisis Kozlakidis, Armen Muradyan, and Karine Sargsyan, 5–12. Cham: Springer, 2024. http://dx.doi.org/10.1007/978-3-031-62332-5.

Marović, Branko, Jovana Vuleta, Zoran Jovanović, and Borislav Panić. "E-Hospital, Children's University Hospital in Belgrade and HELIANT Hospital Information System." *MD Medical Data* 1, no. 4 (2009): 73–77.

Milić, Marko. "Critical Assessment of the HELIANT System in Healthcare in Serbia: Opportunities, Challenges, and Future Directions." Zenodo, December 29, 2024. https://doi.org/10.5281/zenodo.14569252.

Ministry of Health – eHealth Portal. "eSickLeave: Data and Documentation from the Central System," February 6, 2025. Accessed November 29, 2025. https://e-zdravlje.gov.rs/news/ebolovanje-podaci-i-dokumentacija-iz-centralnog-sistema-ebolovanje-4.

Ministry of Health. "User Guide – eHealth Patient Portal." Accessed December 9, 2025. https://e-zdravlje.gov.rs/landing/repository/documents/user-manual-sr.pdf.

NALED. "Annual Report on the Activities and Implementation of NALED's Strategic Goals 2024/25," 2025. https://naled.rs/htdocs/Files/17551/Report-on-Strategic-goals-realization-2024-25.pdf.

NALED. "Report on Activities and Implementation of NALED's Strategic Goals for 2023 and Overview up to 2025," 2024. https://naled.rs/htdocs/Files/14953/Report-on-Strategic-goals-realization-2023-24.pdf.

Nikolić Popadić, Sofija. "Digitalization of Healthcare Services: The Case of Germany." *Glasnik Advokatske Komore Vojvodine* 92, no. 1 (2020): 88–93. https://doi.org/10.5937/gakv92-25688.

Nikolić Popadić, Sofija. "Introducing Telemedicine – Legal and Other Challenges." In *International Scientific Conference: Challenges and Perspectives of the Development of Legal Systems in*

the XXI Century – Conference Proceedings. Banja Luka: Faculty of Law, University of Banja Luka, 2022. Accessed November 8, 2025. http://iriss.idn.org.rs/1290/.

Nikolić Popadić, Sofija, and Marta Sjeničić. "The Use of Artificial Intelligence in Healthcare and Medicine – Legal Aspects." *Journal of Ethics and Legal Technologies* 6, no. 2 (2024): 21–39. https://doi.org/10.14658/pupj-JELT-2024-2-3.

Nikolić Popadić, Sofija, Marko Milenković, and Marta Sjeničić. "The Covid-19 Epidemic in Serbia – The Challenges of Finding an Appropriate Basis for Responding to a Health Crisis." *Medicine, Law & Society* 14, no. 2 (2021). https://doi.org/10.18690/mls.14.2.229-246.2021.

OECD. "Synthesis Report 2025: Health Policy Reform Trends in the EU," 2025. Accessed February 4, 2026. https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/synthesis-report-2025-health-policy-reform-trends-in-the-eu_f661ffc5/1f6a8e9a-en.pdf.

Rajković, Petar, Anđelija Đorđević, Aleksandar Milenković, and Dragan Janković. "The Role of Resource Awareness in Medical Information System Life Cycle." Arxiv (2022). https://arxiv.org/abs/2205.07778.

Reljin, Branimir, and Vojin Ćućuz. "Projekat Telepatološke Mreže." *XXV Simpozijum o Novim Tehnologijama u Poštanskom i Telekomunikacionom Saobraćaju PosTel 2007* (Belgrade), 2007, 101–8.

Secundo, Giustina, S.M. Riad Shams, and Francesco Nucci. "Digital Technologies and Collective Intelligence for Healthcare Ecosystem: Optimizing Internet of Things Adoption for Pandemic Management." *Journal of Business Research* 131 (2021): 563–72. https://doi.org/10.1016/j.jbusres.2021.01.034.

Shanahan, Matthew, and Kalvin Bahia. "The State of Mobile Internet Connectivity 2025: Barriers to Mobile Internet Adoption and Use." GSMA Intelligence, 2025. Accessed February 4, 2026. https://www.gsma.com/somic/wp-content/uploads/2025/11/The-State-of-Mobile-Internet-Connectivity-2025-Barriers-to-Mobile-Internet-Adoption-and-Use.pdf.

Stašević-Karličić, Ivana. "How Much Has the COVID-19 Pandemic Changed Us: The Experience of the Clinic for Mental Disorders 'Dr Laza Lazarević'." *Srpski Medicinski Casopis Lekarske Komore* 2, no. 3 (2021): 295–301. https://doi.org/10.5937/smclk2-33326.

State Audit Institution of the Republic of Serbia. "Performance Audit Report – Information Security in Healthcare Information Systems," 2021. Accessed November 25, 2025. https://www.dri.rs/izvestaj/3410.

Statistical Office of the Republic of Serbia. "The 2022 Census of Population, Households and Dwellings: Educational Attainment, Literacy and Computer Literacy," 2023. Accessed December 13, 2025. https://publikacije.stat.gov.rs/G2023/Pdf/G20234006.pdf.

Statistical Office of the Republic of Serbia. "Use of ICT – Households, 2025," 2025. Accessed December 13, 2025. https://www.stat.gov.rs/sr-latn/vesti/20251024-upotreba-ikt-a-domacinstva-2025/?s=2701.

Stefanović, Milica, ed. *Grey Book of Healthcare*. Belgrade: NALED, 2020. Accessed December 10, 2025. https://naled.rs/htdocs/Files/04612/Siva_knjiga_zdravstva.pdf.

Vekić, Berislav, Filip Pilipović, Viktorija Dragojević-Simić, Rastko Živić, Dragče Radovanović, and Nemanja Rančić. "Implementation of the Nationwide Electronic Health Record System in Serbia: Challenges, Lessons Learned, and Early Outcomes." *Acta Clinica Croatia* 61, no. 3 (2022): 488–95. https://doi.org/10.20471/acc.2022.61.03.14.

World Health Organization. *Global Diffusion of eHealth: Making Universal Health Coverage Achievable. Report of the Third Global Survey on eHealth*. Geneva: World Health Organization, 2016. Accessed February 4, 2026. https://iris.who.int/server/api/core/bitstreams/7349d58e-d87b-4330-ab51-82c75ddbfa62/content.

World Health Organization. "Global Strategy on Digital Health 2020–2025," 2021. Accessed November 10, 2025. https://iris.who.int/server/api/core/bitstreams/1f4d4a08-b20d-4c36-9148-a59429-ac3477/content.

Zajeganović, Marija, Natalija Vugdelija, Radiša Stefanović, Silva Kostić, Uroš Miljković, and George Mach. "Data Security in Mobile Healthcare." *Military Technical Courier* 71, no. 3 (2023): 748–68. https://scindeks-clanci.ceon.rs/data/pdf/0042-8469/2023/0042-84692303748Z.pdf.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 25–38
https://doi.org/10.31743/recl.18702
Received: 5 June 2025 | Accepted: 3 February 2026 | Published: 31 March 2026

Legal Regulation of Electronic Identity in eHealth Services in Poland and Estonia: A Comparative Analysis

Krzysztof Świtała

PhD, Department of Informatics Law, The Law and Administration Faculty, Cardinal Stefan Wyszyński University in Warsaw; correspondence address: Wóycickiego 1/3, 01–938 Warsaw, Poland; e-mail: k.switala@uksw.edu.pl
https://orcid.org/0000-0003-0426-5383

Abstract: The primary aim of the article is to analyze the role of electronic identity in ICT-enabled healthcare in the context of existing legal instruments in these areas, both at the EU level and in the regulations of selected Member States (Poland, Estonia). A basic analysis of eHealth, telemedicine, and EHR systems was conducted, considering the role of electronic identity in data processing within the health care information infrastructure. EU regulations such as eIDAS, the directive on patients' rights in cross-border healthcare, and the regulation on the European Health Data Space were taken into account. The role of electronic identity management systems in the context of the patient's right to medical services, consent, information about their condition, and the preservation of medical professional confidentiality and privacy is also discussed. Finally, existing electronic identification systems in Poland (*Profil Zaufany*, *Profil Osobisty*, *mObywatel*) and Estonia (e-ID), which are also used to authenticate patients accessing healthcare services in these countries, are presented.

Keywords: electronic identity, eHealth, eIDAS, healthcare, EHR

1. Introduction

Modern healthcare is increasingly dependent on information and communication technologies (ICT). The pace of change accelerated, particularly during the COVID-19 pandemic, when the burden of delivering outpatient health services shifted to a remote, decentralized format. Unfortunately, in Poland, these were not comprehensive and mature nationwide telemedicine solutions, but, in practice, only the exchange of voice messages between the patient and doctor via mobile phone services.[1] In the Scandinavian countries, a developed health care system, including modern electronic data processing technologies that incorporate eHealth services and support digitalization efforts, has enabled more effective coping with the challenges of maintaining efficiency and business continuity in this sector.[2] The implementation of ICT in healthcare should complement traditional forms of patient care, taking into account patients' welfare and respecting their rights.

[1] These are the conclusions from an analysis of results from the Ministry of Health and National Health Fund's survey of patient satisfaction with teleconsultations with their primary care physician during the COVID-19 epidemic ("Raport z badania satysfakcji pacjentów korzystających z teleporad u lekarza podstawowej opieki zdrowotnej w okresie epidemii COVID-19" [2020], accessed June 4, 2025, https://www.gov.pl/attachment/a702e12b-8b16-44f1-92b5-73aaef6c165c, 9).

[2] Suhail Muzaik and Nadia Davoody, "Exploring the Operational and Technical Changes in the Healthcare Sector During the COVID-19 Pandemic," in *Telehealth Ecosystems in Practice*, eds. Mauro Giacomini et al. (Amsterdam: IOS Press, 2023), 281.

ISSN 2545-384X (Online)

This article aims to present the legal role of mechanisms for managing and maintaining digital identity in contemporary ICT-enabled healthcare. The analysis will cover existing normative solutions at the EU level and in selected Member States, and will attempt to assess their consistency. To illustrate the issue of electronic identity institutions in the EU, legal solutions introduced by the eIDAS Regulation will be presented. As a use case, electronic identification methods for public and healthcare services in Estonia and Poland will be discussed.

Analysis of the normative material considered in this article was primarily carried out according to the comparative and dogmatic-legal methods, including the presentation and interpretation of legal provisions, a review of the literature on the subject, and the technical standards necessary to elucidate the context of the considerations.

2. eHealth, Telemedicine and EHR

In World Health Organization documents, eHealth is defined as the use of ICT in health care for purposes such as treating patients, conducting research, educating students, detecting disease, and monitoring the health of the population.[3] The scope of this term is not limited to technical and IT issues, but also encompasses other management tools, processes, and working methods that may have a positive impact on patient health and the quality of healthcare services in the information society. The technical standard ISO 27799 defines a concept related to eHealth – a health information system, understood as an electronically maintained health software (intended to be used specifically for managing, maintaining, or improving health of individual persons or the delivery of care – which also covers the adoption of medical devices) and repository of patient personal health information, collected and transmitted securely, and ensuring that these resources are only available to authorized users.[4] The role of identity management modules in ensuring the confidentiality of data processed in eHealth systems is outlined in the analyzed document.

Telemedicine is defined in EU documents as the provision of healthcare services through the use of ICT in situations where the health professional and patient (or group of health professionals) are not in the same location. It involves the secure transmission of medical data and information via text, sound, images, or other forms needed for preventive medicine, diagnosis, treatment, and patient follow-up.[5] Telemedicine solutions enable medical procedures to be performed at a distance (telesurgery), facilitate audio, visual, and text communication between medical specialists (teleconsultation), and enable the remote transmission and description of diagnostic tests (teleradiology) and the remote monitoring of patients (telemonitoring, including telecardiology, telecare).

---

3 "eHealth," World Health Organization. Eastern Mediterranean Region, accessed June 4, 2025, https://www.emro.who.int/health-topics/ehealth/.

4 *ISO 27799 – Health informatics – Information security controls in health based on ISO/IEC 27002* (Geneva: ISO, 2025), 2.

5 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society*, COM(2008) 689 final (Brussels, November 4, 2008), 3.

Electronic Health Records constitute the basic collection of information about patients who receive medical services.[6] Pursuant to § 1(1) of the Ordinance of the Minister of Health of 6 April 2020 on the types, scope, and models of medical records and the manner of their processing,[7] there is an obligation in Poland as of 2019 to keep patient medical records exclusively in electronic form. In accordance with Article 3(m) of Directive 2011/24/EU,[8] medical records mean all the documents containing data, assessments, and information of any kind on a patient's health and clinical evolution throughout the care process. The content of Article 2, point 6 of the Act of 28 April 2011 on the healthcare information system[9] specifies that the EHR consists of documents created in electronic form with a qualified electronic signature, trusted signature, personal signature, or using the method of confirming the origin and integrity of the data available in the ICT system of the Social Insurance Institution (Polish: *Zakład Ubezpieczeń Społecznych*). It should be noted that the definition under consideration emphasizes the importance of using user authentication mechanisms to ensure that EHR processing complies with legal obligations.[10] In EU legislation, the discussed medical records concept is understood as a collection of personal or non-personal electronic health data related to a natural person, collected in the health system and processed for the purpose of providing healthcare (Article 2(2)(j) of Regulation 2025/327). Summarizing the definitions cited above, it can be concluded that the EHR is an appropriately secured set of electronic patient data, constituting a separate, meaningful content and organized in a specific internal structure, processed for the purpose of performing health care tasks. Analysis of the cited definitions leads to the conclusion that eHealth, in fact, encompasses both telemedicine services and EHRs within its scope. Proper functioning of these solutions is not possible without ensuring an adequate level of security covering confidentiality, integrity, authenticity, and accountability for the resources processed in these systems and, mostly, the realization of the rights of their users. This means that electronic identity management systems are a necessary and integral part of this information infrastructure.

3. Electronic Identity

Electronic identity (eID) is a basic component of the knowledge economy and information society.[11] According to ISO 24760–1 technical standard, identity is a set of attributes related to an entity – item relevant for the operation of a domain (environment) that has

6 Urszula Drozdowska et al., *Dokumentacja medyczna* (Warszawa: Eskulap, 2011), 21–22.

7 The Ordinance of the Minister of Health on the types, scope and models of medical records and the manner of their processing of 6 April 2020, Journal of Laws 2024, item 798.

8 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4 April 2011).

9 Act on the healthcare information system of 28 April 2011, Journal of Laws 2025, item 302.

10 Zuzanna Maj, "Elektroniczna dokumentacja medyczna – wybrane aspekty prawne," *Przegląd Prawa Medycznego* 4, no. 1 (2022): 121–22, https://doi.org/10.70537/14y42909.

11 Margarita Robles-Carrillo, "Digital Identity: An Approach to Its Nature, Concept, and Functionalities," *International Journal of Law and Information Technology* 32, no. 1 (2024): 1, https://doi.org/10.1093/ijlit/eaae019.

recognizably distinct existence.[12] Identity is an interdisciplinary issue with political and cultural dimensions that are important from the perspective of legal sciences, especially in the area of human rights.[13] This discussed electronic user authentication solution enables public services to be provided at a distance in a secure, fast, and comprehensive manner, including in the areas of telemedicine and eHealth. It eliminates unnecessary visits to a healthcare provider that are motivated by formal and legal, rather than medical, reasons.

ISO 27002 defines the purpose of identity management as enabling the unique identification of individuals and systems accessing the organization's information and other associated assets, and enabling the appropriate assignment of access rights.[14] It should be noted that, in information technologies, entities with an identity include not only individuals, but also ICT systems and their web services.

In information technology, identification is understood as the process of establishing someone's identity. According to Article 3(1) of the eIDAS,[15] electronic identification means the process of using data in electronic form that uniquely identifies a person or uniquely represents a specific entity (a natural person or legal entity, or a natural person representing a legal entity).

Electronic identity management solutions enable the secure, efficient, and automated management of access to eHealth systems and the resources within them.[16] This makes it possible to further exploit the potential of these tools to improve healthcare quality, while guaranteeing the rights of data subjects and individuals who are recipients of the electronic services offered.

4. EU Legal Solutions

The primary piece of EU legislation on electronic identity is the eIDAS Regulation. From the perspective of the article's subject matter, it regulates electronic signatures, electronic seals, and associated certificates. These solutions are based on electronic data that are attached to, or logically associated with, other electronic data, and which are used by the performer of these activities to ensure the realization of information security attributes, such as authenticity, non-repudiation, accountability, and integrity. The processes

12 *ISO/IEC 24760–1 – Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology* (Geneva: ISO, 2025), 1.

13 Bartosz Liżewski, "The Personal Identity of the Human Being and the Right to Privacy from the Perspective of Standards of the European Court of Human Rights: Theoretical Legal Reflections," *Bialystok Legal Studies* 29, no. 3 (2024): 78–79, https://doi.org/10.15290/bsp.2024.29.03.05.

14 *ISO/IEC 27002 – Information security, cybersecurity and privacy protection – Information security controls* (Geneva: ISO, 2022), 29.

15 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257/73, 28 August 2014).

16 As a part of the technical standards of IHE profiles – recommended in the European Commission decision 2015/1302 of 28 July 2015 on the identification of "Integrating the Healthcare Enterprise" profiles for referencing in public procurement – The Patient Identifier Cross-referencing HL7 Integration Profile (PIXV3) is targeted at cross-enterprise Patient Identifier Cross-reference Domains as well as healthcare enterprises with developed IT infrastructure ("Patient Identifier Cross-referencing HL7 V3 (PIXV3)," Integrating the Healthcare Enterprise, August 4, 2023, accessed February 25, 2026, https://profiles.ihe.net/ITI/TF/Volume1/ch-23.html).

described here, therefore, allow the identity of the entity performing such actions to be declared and reliably confirmed. A certificate is an electronic credential that associates the data used to validate a signature or electronic seal with the entity that uses it. These solutions are, therefore, used to identify natural persons (patients and health professionals) and legal entities (healthcare providers) based on the activities they carry out.

It is worth mentioning that electronic certificates can be used not only to certify the identity of natural persons or legal entities, but also, thanks to the Secure Socket Layer/Transport Layer Security protocol, to ensure the authenticity of websites and web services, as well as the integrity and confidentiality of communications via these solutions. The data structures contained in the certificates in question are mostly compliant with the X.509 standard.[17] The technologies presented here create an interoperable environment for managing electronic identity data.

Cross-border health care using eHealth solutions requires effective methods to manage the identity of those who use them. Activities related to the promotion of universal methods for identifying and authenticating users of healthcare information systems are among the objectives pursued by the eHealth Network, established under Article 14 of Directive 2011/24/EU. One activity undertaken by this consultative and advisory EU body involves issuing recommendations concerning the application of the eIDAS Regulation and eIDs in day-to-day healthcare operations, as well as the use of public registers of persons performing healthcare activities.[18]

In the Regulation 2025/327 on the European Health Data Space,[19] Article 16 indicates that one of the requirements of a secure and interoperable health data processing environment is to ensure that data users only have access to the electronic health data which they are authorized to access, and only by means of individual and unique user identities and confidential modes. Moreover, regarding medical professionals using priority categories of electronic personal health data (patient summaries, electronic prescriptions and dispensations, medical imaging studies, and related imaging reports), the requirements for their use of eIDAS-compliant electronic identification means are set out in Article 12 of the EHDS. Ensuring accountability for access to medical databases should be based on effective, legally recognized user authentication mechanisms that guarantee the realization of fundamental rights, such as privacy and the informational autonomy of the individual.

It should be added that the introduction of the legal act under consideration is to be coupled with the implementation of data controller obligations related to the implementation of new mechanisms for the electronic identification of patients, health professionals,

---

17 Diana Gratiela Berbecaru and Antonio Lioy, "An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem," *IEEE Access* 11 (2023): 79160, https://doi.org/10.1109/ACCESS.2023.3299357.

18 European *eHealth Network*, *Recommendation Paper on Policies Regarding eIDAS eID and Health Professional Registries* (Brussels: European *eHealth Network*, May 15, 2018), accessed June 3, 2025, https://health.ec.europa.eu/system/files/2018-09/ev_20180515_co11b_en_0.pdf.

19 Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (OJ L 327, 5 March 2025).

and researchers, including in relation to the digital identity wallet.[20] The concepts for new regulations in this area were laid out in the eIDAS amendment, which extended harmonization and improved the security of trust services.[21] Regulation 2024/1183 of the European Parliament and of the Council of 11 April 2024, amending Regulation No. 910/2014 as regards establishing the European Digital Identity Framework,[22] introduces a normative definition of the concept of a European Digital Identity Wallet, which is a product and service that enables a user to store identity data, credentials, and attributes associated with their identity, provide them on demand to relevant parties, and use them for online and offline authentication.[23] The presented solution is a universal, secure, and reliable tool for managing personal electronic identification facilities.[24]

The dispersion of eID regulation across the EU internal market and healthcare legislation creates a significant risk of inconsistencies in the normative solutions established. The eHealth Network, Data Protection Authorities, and ENISA have a particular role in flagging potential gaps and conflicts to ensure the cybersecurity of solutions introduced and subsequently applied throughout their lifecycle.

5. Patient Rights and Electronic Identification in Healthcare

The patient's right to health services in accordance with current medical knowledge also includes the use of modern techniques for the electronic processing of medical data, in particular for teleconsultation or diagnostic imaging.[25] Electronic identity has a significant impact on increasing the accessibility of eHealth systems for people with reduced mobility, hearing, or visual impairments. It is impossible not to mention here Directive 2016/2102,[26] the implementation of which in the legal order of EU Member States creates the necessary legal requirements in the area under consideration, which also apply to a significant part of healthcare entities. Their adoption by healthcare providers in the EU is

[20] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847, recital 21.

[21] European Commission, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*, COM(2021) 281 final (Brussels, June 3, 2021), 281.

[22] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (OJ L 1183, 30 April 2024).

[23] In Poland, the adoption of the European digital identity wallet concept was proposed in a draft bill amending the Act on Trust Services and Electronic Identification and certain other acts (RCL No. UC122 of 18 February 2026).

[24] Julián Inza, "The European Digital Identity Wallet as Defined in the EIDAS 2 Regulation," in *Governance and Control of Data and Digital Economy in the European Single Market: Legal Framework for New Digital Assets, Identities and Data Spaces*, ed. Carmen Pastor Sempere (Cham: Springer, 2025), 440.

[25] Dorota Karkowska, "Prawo pacjenta do świadczeń zdrowotnych (art. 6)," in *Prawa pacjenta i Rzecznik Praw Pacjenta. Komentarz*, ed. Dorota Karkowska (Warsaw: Wolters Kluwer, 2021), 232–392.

[26] Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (OJ L 327, 2 December 2016).

often insufficient.[27] Solutions that implement digital accessibility standards (e.g., the Web Content Accessibility Guidelines) in eHealth systems can offer better-tailored access to health information and medical records, including diagnostic test results.[28]

Dynamic adaptation of user access conditions in specific data-processing circumstances is possible due to the layering (content, structure, and visualization) and modularity of electronic documents (division into sections), which are completely independent of the medium (data storage) on which they are processed. A document can therefore be dynamically divided into sections without affecting its structure. This facilitates the visualization of individual sections adapted to the specific recipient. It is also possible to hide certain information from a user who lacks the necessary rights to access it lawfully.

Using digital identity solutions, patients can consent to both telemedicine and traditional services. This makes it easier to read the information about the procedure and allows such a statement of intent to be expressed anywhere, anytime. The patient is not obliged to collect the relevant paper form in advance and, once signed, to physically deliver it before the medical procedure begins.

The patient's right to health information and the right of access to electronic records can be realized through ICT. They are significantly intertwined in terms of subject matter (information) and object (patients and health professionals). The right to medical records is the de facto basis for the realization of the right to health information, as it serves as the designated collection of patient data regarding the treatment process.[29] These rights guarantee an appropriate degree of autonomy and subjectivity to the patient, and enable him to make genuinely voluntary decisions in healthcare.[30] The right of access to medical records and the right to be informed about one's health facilitate informed consent, understood as an informed act, made by the patient or the patient's legal representative, freely chosen and clearly expressed, based on coherent, reliable information about all stages of the medical procedure.[31] A person who is comprehensively and precisely informed about their health condition can become an aware participant in healthcare processes.

Electronic identity, in the context of the right to privacy and the physician–patient privilege, enables the confidentiality of patient-related information. This assumption is made possible by pursuing authenticity and accountability as part of data processing activities. Methods for identifying, authenticating, and authorizing users of eHealth and EHR systems enable the recording of which actions have been performed and when.

---

27 Marika Jonsson et al., "How Have Public Healthcare Providers in Sweden Conformed to the European Union's Web Accessibility Directive Regarding Accessibility Statements on Their Websites?," *Universal Access in the Information Society* 24 (2025): 456, https://doi.org/10.1007/s10209-023-01063-1.

28 Gloria Acosta-Vargas et al., "Improvement of Accessibility in Medical and Healthcare Websites," in *Advances in Human Factors and System Interactions: Proceedings of the AHFE 2021 Virtual Conference on Human Factors and Systems Interaction, July 25–29, 2021, USA*, ed. Isabel L. Nunes (Cham: Springer, 2021), 266–73.

29 Izabela Bernatek-Zaguła, *Prawo pacjenta w Polsce do informacji medycznej* (Toruń: Wydawnictwo Adam Marszałek, 2008), 93.

30 Tomasz Pietrzykowski and Katarzyna Smilowska, "The Reality of Informed Consent: Empirical Studies on Patient Comprehension – Systematic Review," *Trials* 22, no. 57 (2021): 7–8, https://doi.org/10.1186/s13063-020-04969-w.

31 Małgorzata Świderska, *Zgoda Pacjenta na zabieg medyczny* (Toruń: Dom Organizatora TNOiK, 2007), 19.

If these processes fail, an unauthorized person should not have access to the protected resources. The use of adequate safeguards to address a constantly evolving catalog of threats is particularly important for protecting data processed in healthcare using ICT.[32] It is worth noting that access control is one of the areas indicated in ISO 27001 requirements for Information Security Management Systems.[33] The use of appropriately clear and effective legal and technical mechanisms to restrict access to patient data only to genuinely justified cases of use, taking into account the necessity and proportionality of the measures taken, should be the standard for managing processable resources in the health information system.[34] With regard to medical confidentiality, the user authentication mechanisms discussed here help protect the patient's autonomy by effectively identifying those authorized to access their health data. The right to informational self-determination through the use of the technical and organizational access management solutions discussed here can be adequately preserved in this case.[35] Effective data exchange in healthcare that guarantees confidentiality, integrity, authenticity, non-repudiation, and accountability is an important factor in ensuring that the quality of services provided meets the needs while maintaining the level of trust in the doctor–patient relationship.

The use of properly functioning electronic services for the management of user identity in e-Health systems is closely linked to the respect of patient rights. This allows these legal obligations to be implemented in the electronic processing of medical data and to ensure an appropriate degree of autonomy for data subjects.

6. The Estonian Electronic Identification System

At the beginning of the 21st century, Estonia's information infrastructure for electronic data processing was among the best developed in Europe.[36] Its foundation is X-Road – an ICT environment for unified and secure data exchange between private and public-sector organizations across the country.[37] Part of the nationwide information infrastructure is the Estonian Electronic Identification System (e-ID), consisting of the following elements:

– ID card (chapter 5 "Identity Card" – § 19 – § 20),
– Residence Permit card (chapter 7 "documents held by aliens" – § 34^1 – § 34^3),

[32] Bożena Skubis, "Ochrona danych medycznych w okresie pandemii COVID-19. Działania Rzecznika Praw Pacjenta dotyczące prawa do dokumentacji medycznej i tajemnicy informacji w latach 2020–2022," *Przegląd Prawa Medycznego* 6, no. 3 (2024): 61, https://doi.org/10.70537/vmgpq521.

[33] *ISO/IEC 27001 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements* (Geneva: ISO, 2022), 12.

[34] Robert Pudlo, Małgorzata Pudlo, and Marcin Burdzik, "Medical Confidentiality in the Polish Legal System: A Real or Illusory Instrument of Patient Privacy Protection?," *Psychiatria Polska* 58, no. 5 (2024): 902–03, https://doi.org/10.12740/pp/onlinefirst/166174.

[35] Sabine Michalowski, *Medical Confidentiality and Crime* (Aldershot: Ashgate, 2003), 12–13.

[36] Edwin Bendyk, "Web 2.0 – sposób na modernizację administracji z udziałem obywateli," *Elektroniczna Administracja*, no. 1 (2008): 53.

[37] Karoline Paide et al., "On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships," in *ICEGOV '18: Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, eds. Atreyi Kankanhalli, Adegboyega Ojo, and Delfina Soares (New York: ACM, 2018), 34.

- Digi-ID (chapter 5^1 "Digital Identity Card" – § 20^1 – § 20^3),
- e-Residency Digi-ID (chapter 5^2 "e-Resident's Digital Identity Card" – § 20^5 – § 20^{12}),
- Mobiil-ID (chapter 5^1 "Digital Identity Card" – § 20^3 – § 20^4),
- Diplomatic identity card (chapter 5^3 "Diplomatic Identity Card" – § 20^{13} – § 20^{16}).

The functionalities described are widely used in the domestic legal environment, not only to identify individuals and determine their eligibility for health insurance and access to health services or medical records, but also for administrative procedures, public registers, banking services, public transport, social benefits, and general elections (voting).[38] The legal basis for these solutions is the Identity Documents Act (Estonian: *Isikut tõendavate dokumentide seadus*) passed in 1999.[39] The concept of electronic identity corresponds most closely to Digi-ID. This tool allows a specific person to be identified solely in an electronic (digital) environment and thus to use the assigned services.[40] In other cases, we are in fact dealing with hybrid solutions that can be used for analogue, stationary activities (Information System Authority, ID card). It should be added that the Health Services Organisation Act (Estonian: *Tervishoiuteenuste korraldamise seadus*), applied since 2002, implies the use of the e-ID solutions for healthcare (chapter 5^1 "Health Information System" – § 59^1 – § 59^4).[41]

An interesting solution is Mobiil-ID, which verifies a person's identity using the mobile device and the data stored on its SIM card (Information System Authority, Mobile-ID). This method of identification bears similarities to the Polish system for identifying people via the *mObywatel* (mCitizen) application, which will be described in more detail later in this article.

The electronic identity solutions described are used within the Estonian healthcare system, which relies heavily on ICT. The e-Health solutions operating in Estonia are among the most mature in the European Union, as evidenced by the implementation of electronic access services for citizens, categories of accessible health data, access technologies, and coverage and access opportunities for certain categories of people.[42] According to data from as early as 2011, 84% of prescriptions generated under this system were electronic.[43] In addition to this functionality, the national eHealth system (Estonian: *Terviseportaal*) also enables enrolment in health services, access to patients' medical records, teleconsultation, and full processing of laboratory test and diagnostic imaging

38 Kamil Czaplicki, *Dokumenty tożsamości. Jawność i bezpieczeństwo* (Warsaw: C.H. Beck, 2016), 310.

39 It also includes rules on travel documents (chapter 6), including Estonian citizens' passports (§ 21). In Poland, this issue is covered by a special law of January 27, 2022 on passport documents (Journal of Laws 2024, item 1063).

40 Piia Tammpuu et al., "Estonian e-Residency and Conceptions of Platform-Based State Individual Relationship," *Trames Journal of the Humanities and Social Sciences* 26, no. 1 (2022): 7, https://doi.org/10.3176/tr.2022.1.01.

41 In Poland, the rules governing the operation of national e-Health systems are set out separately in the Act on the healthcare information system.

42 Estonia achieved a 100% score in the 2024 eHealth maturity scores report and ranked first. Poland, with a score of 92%, ranked sixth (Martin Page and Puck de Waal, *2025 Digital Decade eHealth Indicator Study: Executive Summary* [Luxembourg: Publications Office of the European Union, 2025], 8, https://data.europa.eu/doi/10.2759/0682933).

43 Taavi Lai et al., "Estonia: Health System Review," *Health Systems in Transition* 14, no. 6 (2013): 103.

data.[44] The wide range of functionality, along with consistency and interoperability with other electronic services, including e-ID, puts the Estonian health care information system at the forefront in Europe in terms of the development and comprehensive use of ICT capabilities.

7. Electronic Identification Solutions in Poland

The Polish Public Electronic Identification System, until April 19, 2023, includes two means of identification: a trusted profile (Polish: *Profil Zaufany*) and a personal profile (Polish: *Profil Osobisty*).[45] Pursuant to Article 3, point 14 of the Act of 17 February 2005 on the computerization of the activities of entities performing public tasks,[46] the trusted profile contains data that identifies and describes a natural person, which was issued in accordance with the provisions of the law, while pursuant to Article 2, paragraph 1, point 10 of the Act of 6 August 2010 on identity cards,[47] the personal profile includes data confirmed by a certificate, which is an electronic attestation used to identify and authenticate the holder of an identity card confirming the data of that person. These solutions can be used in user authentication for services within the healthcare information system, such as the Internet Patient Account (Polish: *Internetowe Konto Pacjenta*, pacjent.gov.pl)[48] and eGabinet (gabinet.gov.pl) for medical professionals.

mCitizen (Polish: *mObywatel*) is a mobile application that provides electronic documents as digital services. An *mObywatel* document is a mobile document (i.e., an electronic document supported by a service made available through the *mObywatel* application) confirming the identity and citizenship of Poles and other residents. The legal basis for this means of identification is the Act of 26 May 2023 on the *mObywatel* application.[49] Although this service, as a rule, can only be used in traditional, stationary contacts with medical entities, the identification data is in electronic form. Moreover, an *mObywatel* profile is a designated authentication tool for users of public ICT systems.

De lege ferenda, efforts should be made to integrate these Polish Public Electronic Identification System services with both the electronic delivery system[50] and mo-

44 Kaija Kasekamp et al., "Estonia: Health System Review," *Health Systems in Transition* 25, no. 5 (2023): 26.

45 Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ C 2836, 22 April 2024).

46 Act on the computerization of the activities of entities performing public tasks of 17 February 2005, Journal of Laws 2024, item 1557.

47 Act on identity cards of 6 August 2010, Journal of Laws 2022, item 671.

48 It should be noted that the electronic Health Insurance Card provided for in Article 49 of the Act of 27 August 2004 on healthcare services financed from public funds (Journal of Laws 2024, item 146), which could potentially be used to identify patients in the healthcare system, is not currently being issued (Andrzej Sidorko, "Karta ubezpieczenia zdrowotnego i inne dokumenty potwierdzające prawo do świadczeń [art. 49]," in *Ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Komentarz*, ed. Agnieszka Pietraszewska-Macheta, 4th ed. [Warsaw: Wolters Kluwer, 2023], 491–93, LEX/el).

49 Act on the *mObywatel* application of 26 May 2023, Journal of Laws 2024, item 1275.

50 The issue of exchange of correspondence with public entities in Poland is comprehensively regulated by the Act of 18 November 2020 on electronic delivery (Journal of Laws 2024, item 1045). The electronic registered delivery service provided for therein is a trust service within the meaning of eIDAS. The proper functioning

bile *mObywatel* services, so that they are consistent in terms of legal construction and technical requirements, and do not raise doubts about their interoperability and scope of application. The public identification services operating in Poland – unlike in Estonia – are characterized by too much dispersion and are not fully compatible.

8. Conclusions

The use of electronic data processing technologies is becoming widespread. In addition to their collection, editing, and reading, they are increasingly subject to complex statistical analyses and are becoming a resource for Machine Learning and Artificial Intelligence algorithms. These challenges also apply to the healthcare system. The aging of European populations and the resulting growing demand for healthcare services, coupled with a lack of medical professionals relative to current needs, make the use of eHealth solutions indispensable for maintaining the quality of healthcare services. The increasing interoperability and potential for using information resources in this sector are closely correlated with the development of evidence-based medicine.

In an ever more digitalized world, electronic identity management mechanisms are becoming more important, including in healthcare, which is increasingly using eHealth systems to deliver healthcare services. The legal solutions in this area are still being optimized to address the technical and social challenges of the coming decades. During this process, it is crucial to ensure the privacy and information autonomy of individuals, while exploiting the full potential of modern data processing techniques – without unjustifiably interfering with fundamental rights. These processes are carried out to extract as much useful information as possible, as well as a range of valuable knowledge from these resources, to understand better the reality around us, especially with respect to healthcare and support for decision-making.

The issue of user identification in eHealth systems, discussed in this article, concerns the authentication process, which verifies the identity of the specific person. Establishing the user's identity allows, as part of the next authentication phase, to allocate them a range of access to protected information resources, commensurate with their level of privileges in the ICT system. This therefore allows the legal requirements related to the protection of personal data and the secrets of the medical profession from unauthorized access by unauthorized persons to be realized.

In the case of the methods used to identify individuals in Estonia, a logical division has been adopted between physical identity documents with an electronic layer (ID cards) and digital identities (Digi-ID), and mobile profiles (Mobiil-ID), operated exclusively in electronic form, the latter via mobile devices. A similar concept has been adopted in Poland, assuming the existence of an identity card with an electronic personal profile, a trusted profile and an m-Citizen profile. However, regulations concerning electronic identification in Poland are scattered across many legal acts (the ID Card Act, the Computerisation Act, the *mObywatel* Application Act, the Electronic Delivery Act).

of health care is based not only on the implementation of clinical activities, but also on effective management processes involving interactions with public entities.

In Estonia, on the other hand, this issue has been unified in a single act, the Identity Documents Act. In addition, the national Public Electronic Identification System, which complies with the requirements of Article 9(1) of eIDAS, consists of all the comprehensive methods of authenticating natural persons in Estonia mentioned in this article (ID card, RP card, Digi-ID, e-Residency Digi-ID, Mobiil-ID, Diplomatic identity card), while in Poland it consists only of Trusted profile and Personal profile (linked to the Identity Card), without including the identification functionality in the *mObywatel* application. The Estonian approach, which assumes uniformity of the solutions adopted – both in the sphere of legal instruments and technical solutions – is more coherent and mature. This consideration applies to both the normative and technical/implementation layers, based on the integration of electronic identification services.

The proper functioning of health care based on electronic data processing and eHealth requires secure, trusted user identity management services and proven mechanisms for managing access to protected health information resources. The importance of consistent and effective regulation in this area, supported by non-legal instruments such as technical standards and soft law – especially internal organizational policies and codes of conduct – cannot be overstated.

References

Acosta-Vargas, Gloria, Patricia Acosta-Vargas, Janio Jadán-Guerrero, Luis Salvador-Ullauri, Mario Gonzalez. "Improvement of Accessibility in Medical and Healthcare Websites." In *Advances in Human Factors and System Interactions: Proceedings of the AHFE 2021 Virtual Conference on Human Factors and Systems Interaction, July 25–29, 2021, USA*, edited by Isabel L. Nunes, 266–73. Cham: Springer, 2021.

Bendyk, Edwin. "Web 2.0 – sposób na modernizację administracji z udziałem obywateli." *Elektroniczna Administracja*, no. 1 (2008): 53.

Berbecaru, Diana Gratiela, and Antonio Lioy. "An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem." *IEEE Access* 11 (2023): 79156–75. https://doi.org/10.1109/ACCESS.2023.3299357.

Bernatek-Zaguła, Izabela. *Prawo pacjenta w Polsce do informacji medycznej*. Toruń: Wydawnictwo Adam Marszałek, 2008.

Coggon, John, and José Miola. "Autonomy, Liberty, and Medical Decision-Making." *Cambridge Law Journal* 70, no. 3 (2011): 523–47.

Czaplicki, Kamil. *Dokumenty tożsamości. Jawność i bezpieczeństwo*. Warsaw: C.H. Beck, 2016.

Drozdowska, Urszula, Ewa Kowalewska-Borys, Arkadiusz Bieliński, and Wojciech Wojtal. *Dokumentacja medyczna*. Warszawa: Eskulap, 2011.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society*. COM(2008) 689 final. Brussels, November 4, 2008.

European Commission. *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*. COM(2021) 281 final. Brussels, June 3, 2021.

European Commission. *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*. COM(2022) 197 final. Brussels, May 3, 2022.

European *eHealth Network*. *Recommendation Paper on Policies Regarding eIDAS eID and Health Professional Registries*. Brussels: European *eHealth Network*, May 15, 2018. Accessed June 3, 2025. https://health.ec.europa.eu/system/files/2018-09/ev_20180515_co11b_en_0.pdf.

Integrating the Healthcare Enterprise. "Patient Identifier Cross-Referencing HL7 V3 (PIXV3)," August 4, 2023. Accessed February 25, 2026. https://profiles.ihe.net/ITI/TF/Volume1/ch-23.html.

Inza, Julián. "The European Digital Identity Wallet as Defined in the EIDAS 2 Regulation." In *Governance and Control of Data and Digital Economy in the European Single Market: Legal Framework for New Digital Assets, Identities and Data Spaces*, edited by Carmen Pastor Sempere, 433–52. Cham: Springer, 2025.

ISO 27799 – Health informatics – Information security controls in health based on ISO/IEC 27002. Geneva: ISO, 2025.

ISO/IEC 24760–1 – Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology. Geneva: ISO, 2025.

ISO/IEC 27001 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022.

ISO/IEC 27002 – Information security, cybersecurity and privacy protection – Information security controls. Geneva: ISO, 2022.

Jonsson, Marika, Catharina Gustavsson, Jan Gulliksen, and Stefan Johansson. "How Have Public Healthcare Providers in Sweden Conformed to the European Union's Web Accessibility Directive Regarding Accessibility Statements on Their Websites?." *Universal Access in the Information Society* 24 (2025): 449–62. https://doi.org/10.1007/s10209-023-01063-1.

Karkowska, Dorota. "Prawo pacjenta do świadczeń zdrowotnych (art. 6)." In *Prawa pacjenta i Rzecznik Praw Pacjenta. Komentarz*, edited by Dorota Karkowska, 232–392. Warsaw: Wolters Kluwer, 2021.

Kasekamp, Kaija, Triin Habicht, Andres Võrk, Kristina Köhler, Marge Reinap, Kristiina Kahur, Heli Laarmann, and Yulia Litvinova. "Estonia: Health System Review." *Health Systems in Transition* 25, no. 5 (2023): 1–236.

Lai, Taavi, Triin Habicht, Kristiina Kahur, Marge Reinap, Raul Kiivet, Ewout van Ginneken. "Estonia: Health System Review." *Health Systems in Transition* 14, no. 6 (2013): 1–196.

Liżewski, Bartosz. "The Personal Identity of the Human Being and the Right to Privacy from the Perspective of Standards of the European Court of Human Rights: Theoretical Legal Reflections." *Bialystok Legal Studies* 29, no. 3 (2024): 77–90. https://doi.org/10.15290/bsp.2024.29.03.05.

Maj, Zuzanna. "Elektroniczna dokumentacja medyczna – wybrane aspekty prawne." *Przegląd Prawa Medycznego* 4, no. 1 (2022): 121–22. https://doi.org/10.70537/14y42909.

Michalowski, Sabine. *Medical Confidentality and Crime*. Aldershot: Ashgate, 2003.

Muzaik, Suhail, and Nadia Davoody. "Exploring the Operational and Technical Changes in the Healthcare Sector During the COVID-19 Pandemic." In *Telehealth Ecosystems in Practice*, edited by Mauro Giacomini et al., 277–81. Amsterdam: IOS Press, 2023.

Page, Martin, and Puck de Waal. *2025 Digital Decade eHealth Indicator Study: Executive Summary*. Luxembourg: Publications Office of the European Union, 2025. https://data.europa.eu/doi/10.2759/0682933.

Paide, Karoline, Ingrid Pappel, Heiko Vainsalu, and Dirk Draheim. "On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships." In *ICEGOV '18: Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, edited by Atreyi Kankanhalli, Adegboyega Ojo, and Delfina Soares, 34–41. New York: ACM, 2018.

Pietrzykowski, Tomasz, and Katarzyna Smilowska. "The Reality of Informed Consent: Empirical Studies on Patient Comprehension – Systematic Review." *Trials* 22, no. 57 (2021): 7–8. https://doi.org/10.1186/s13063-020-04969-w.

Pudlo, Robert, Małgorzata Pudlo, and Marcin Burdzik. "Medical Confidentiality in the Polish Legal System: A Real or Illusory Instrument of Patient Privacy Protection?." *Psychiatria Polska* 58, no. 5 (2024): 895–907. https://doi.org/10.12740/pp/onlinefirst/166174.

"Raport z badania satysfakcji pacjentów korzystających z teleporad u lekarza podstawowej opieki zdrowotnej w okresie epidemii COVID-19" (2020). Accessed June 4, 2025. https://www.gov.pl/attachment/a702e12b-8b16-44f1-92b5-73aaef6c165c.

Robles-Carrillo, Margarita. "Digital Identity: An Approach to Its Nature, Concept, and Functionalities." *International Journal of Law and Information Technology* 32, no. 321 (2024): eaae019. https://doi.org/10.1093/ijlit/eaae019.

Sidorko, Andrzej. "Karta ubezpieczenia zdrowotnego i inne dokumenty potwierdzające prawo do świadczeń (art. 49)." In *Ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Komentarz*, edited by Agnieszka Pietraszewska-Macheta, 4th ed., 491–93. Warsaw: Wolters Kluwer, 2023. LEX/el.

Skubis, Bożena. "Ochrona danych medycznych w okresie pandemii COVID-19. Działania Rzecznika Praw Pacjenta dotyczące prawa do dokumentacji medycznej i tajemnicy informacji w latach 2020–2022." *Przegląd Prawa Medycznego* 6, no. 3 (2024): 50–74. https://doi.org/10.70537/vmgpq521.

Świderska, Małgorzata. *Zgoda Pacjenta na zabieg medyczny*. Toruń: Dom Organizatora TNOiK, 2007.

Tammpuu, Piia, Anu Masso, Mergime Ibrahimi, and Tam Abaku. "Estonian e-Residency and Conceptions of Platform-Based State Individual Relationship." *Trames Journal of the Humanities and Social Sciences* 26, no. 1 (2022): 3–21. https://doi.org/10.3176/tr.2022.1.01.

World Health Organization. Eastern Mediterranean Region. "eHealth." Accessed June 4, 2025. https://www.emro.who.int/health-topics/ehealth/.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 39–51
https://doi.org/10.31743/recl.18727
Received: 15 June 2025 | Accepted: 3 March 2026 | Published: 31 March 2026

The Scope of Piercing the Corporate Veil in a Limited Liability Company in Georgia: A Comparative Analysis of German and Georgian Law

Simon Takashvili

PhD, Affiliated Associate Professor, Doctor of Law, Sulkhan-Saba Orbeliani University; correspondence address: 3, K. Kutateladze Str., 0186, Tbilisi, Georgia; e-mail: s.takashvili@sabauni.edu.ge
https://orcid.org/0000-0001-8608-170X

Tinatin Peikrishvili

PhD Candidate, Invited Lecturer, Faculty of Law, Sulkhan-Saba Orbeliani University; correspondence address: 3, K. Kutateladze Str., 0186, Tbilisi, Georgia; e-mail: tinatin.feiqrishvili@sabauni.edu.ge
https://orcid.org/0009-0005-9457-0956

Salome Koberidze

PhD Candidate, Affiliated Assistant, Sulkhan-Saba Orbeliani University; correspondence address: 3, K. Kutateladze Str., 0186, Tbilisi, Georgia; e-mail: s.koberidze@sabauni.edu.ge
https://orcid.org/0009-0000-1799-4126

Giorgi Chikviladze

PhD Candidate in Law, Faculty of Law, Sulkhan-Saba Orbeliani University; correspondence address: 3, K. Kutateladze Str., 0186, Tbilisi, Georgia; e-mail: giorgi.chikviladze@sabauni.edu.ge
https://orcid.org/0009-0000-3598-5629

Abstract: Under the Association Agreement, Georgia undertook the obligation to harmonize its legislation with EU legal standards. This commitment is reflected in the Law of Georgia "On Entrepreneurs," adopted in 2022. The new law offers regulation on corporate veil piercing, but, due to its novelty, Georgian judicial practice and doctrinal interpretations are still very scarce for establishing a legal standard. The article examines the legal framework of piercing the corporate veil in Georgian law through a comparative analysis with German law. Although the corporate veil traditionally protects shareholders from personal liability, both the Georgian and German legal systems recognize exceptions in which this protection may be disregarded. Georgian law establishes two cumulative preconditions for piercing the corporate veil: abuse of the legal form and the company's inability to satisfy creditors. The Supreme Court of Georgia has identified indicators of such abuse, including the "alter ego" doctrine, commingling of assets, and undercapitalization. At the same time, the article examines the relationship between tort and corporate liability, addressing the potential competition of legal remedies available to creditors when imposing personal liability on shareholders. The research aims to contribute to the development of Georgian judicial practice by analyzing the doctrine of piercing the corporate veil and its role in strengthening creditor protection and corporate accountability.

Keywords: veil pierce, shareholder, personal liability, abuse, legal form, assets

1. Introduction

Traditional corporate law is based on the concept of a corporation's separate legal personality, under which the company is distinct from its shareholders and possesses its own

ISSN 2545-384X (Online)

structure, rights, and obligations.[1] Shareholders of a limited liability company are generally not liable for the company's debts, and only the company's assets are available to creditors.[2] However, this principle is neither absolute nor unconditional. In certain circumstances, the strict separation between shareholders' assets and the company's assets is not justified.[3] This exceptional case is addressed by the so-called doctrine of piercing the corporate veil recognized in corporate law, pursuant to which shareholders may be held personally liable to creditors under certain conditions.[4] Piercing the corporate veil may occur where shareholders misuse the corporate form, evade legal obligations, or otherwise engage in conduct that undermines the purpose of limited liability,[5] either at the stage of the company's formation or during its subsequent operation.[6]

This research aims to identify the preconditions for piercing the corporate veil under Georgian law through comparative analysis with German law, determine the scope of shareholders' personal liability and examine the available legal remedies and mechanisms for exercising creditors' rights.

This research is significant and relevant because of the paucity of research on the personal liability of limited liability company shareholders under the corporate veil doctrine in Georgian legal literature and practice. This issue becomes particularly important because Article 26 of the law of Georgia "On Entrepreneurs," which regulates piercing the corporate veil, does not provide a specific list of situations or criteria in which such liability arises, referring only to the abuse of the legal form of the company.[7] In the absence of such statutory guidance, legal scholarship and judicial practice play a crucial role in clarifying the scope and application of the doctrine. Due to the limited literature and practice, Georgian courts rely on foreign legal approaches to ground decisions on piercing the corporate veil. At the same time, a partner's personal liability may arise under both tort law and the Law of Georgia "On Entrepreneurs," creating a competition between different legal mechanisms. Accordingly, this research analyzes the approaches of Georgian law and judicial practice through comparative analysis with German law, aiming to contribute to the proper development of Georgian judicial practice. This is especially important nowadays, because the Law "On Entrepreneurs," which entered into

1 Karen Vandekerckhove, *Piercing the Corporate Veil: A Transnational Approach* (Alphen aan den Rijn: Kluwer Law International, 2007), 3–4.

2 Gerard Wirth et al., *Corporate Law in Germany*, 4th ed. (München: C.H. Beck, 2024), 23.

3 Klaus J. Müller, *The GmbH: A Guide to the German Limited Liability Company*, 3rd ed. (München: C.H. Beck, 2016), 93.

4 Decision of the Supreme Court of Georgia of 21 February 2025 No. ას-474–2024.

5 Giorgi Ustiashvili, "Corporate Veil Piercing – In the Doctrine of Georgian, German, and U.S. Law," in *Sergo Jorbenadze 90*, ed. Sergo Jorbenadze (Tbilisi: Sulkhan-Saba Orbeliani University, 2019), 141.

6 Jean-Marie Nelissen Grade and Matthias Wauters, "Reforming Legal Capital: Harmonisation or Fragmentation of Creditor Protection?," in *The European Company Law Action Plan Revisited: Reassessment of the 2003 Priorities of the European Commission*, eds. Koen Geens and Klaus J. Hopt (Leuven: Leuven University Press, 2010), 47.

7 Law of Georgia "On Entrepreneurs," Article 26(2).

force on January 1, 2022,[8] is based on the guiding directions of the European Union under the Association Agreement.[9]

This article consists of six parts, of which the first section provides the introduction to the research. The second section identifies the legal basis for piercing the corporate veil. The third section examines the abuse of the company's legal form. In contrast, the fourth section outlines the preconditions for the company's inability to satisfy creditors, which constitutes a prerequisite for piercing the corporate veil. Therewith, the fifth section addresses the potential competition of creditor legal remedies when imposing personal liability on shareholders. The final section contains the conclusion.

2. Legal Basis for Piercing the Corporate Veil

As mentioned above, the legal basis for imposing personal liability on a shareholder is provided in the Law of Georgia "On Entrepreneurs." Along with the evolution of the latter, the article regulating piercing the corporate veil was amended. Within the existing regulatory framework, the legislation allows for piercing the corporate veil if shareholders abuse the legal form of limited liability and if the company cannot satisfy the creditors' claims, as it is evident that Georgian legislation fails to define abuse of legal form. However, unlike the previous statutory regime,[10] it imposes a second precondition: the company must satisfy its creditors before imposing personal liability on the shareholder. Moreover, before assessing the element of abuse of legal form, the court must establish the company's insolvency.[11] It should not be overlooked that, according to the opinion expressed in the literature, in order to determine personal liability of a shareholder, the result of abuse of legal form should be such a deterioration of the financial condition of the company that it cannot satisfy the creditor's claim.[12]

In contrast to Georgian law, the concept of piercing the corporate veil has no statutory basis in German law. According to the legal doctrine, the term may refer to situations in which shareholders incur personal liability for the company's debts towards its creditors.[13] According to judicial practice, the following circumstances were regarded as possible exceptions to the limited liability concept: commingling of assets, the use of the company as a mere facade (for example, to commit fraud or other wrong), undercapitalization,[14] and confusion of business activities. These are the most common cases

8 New law of Georgia "On Entrepreneurs" was enacted on January 1, 2022; prior to that, the law of Georgia "On Entrepreneurs," enacted on October 28, 1994, was in force.

9 Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Georgia, of the other part (OJ L 261, 30 August 2014), 4–743.

10 Law of Georgia No. 240.000.000.05.001.000.087 of 28 October 1994 on Entrepreneurs, Article 3(6).

11 Irakli Burduli et al., *Corporate Law* (Tbilisi: World of Lawyers, 2022), 391.

12 Giorgi Giguashvili and Giorgi Jugheli, *Commentary on the Law of Georgia on Entrepreneurs* (Tbilisi: Investor Council Secretariat, 2022), 62.

13 Mariusz Fras, "The Doctrine of Veil-Piercing Liability in Poland and Selected Countries: A Comparative Law Study," *Journal of Civil Law Studies* 14, no. 1 (2022): 110.

14 Christian Jungmann and Daniele Santoro, *German GmbH Law: Das deutsche GmbH-Recht*, 2nd ed. (München: C.H. Beck, 2020), 34.

of piercing the corporate veil.[15] The concept of using the analogy to pierce the corporate veil doctrine was established in the case law of the Federal Court of Justice (*Bundesgerichtshof*) from 2001 to 2009. German courts established that shareholders are liable for damages and losses caused by an infringement that endangers the company's survival by draining indispensable financial resources.[16] A situation arises when a shareholder withdraws from the company, leaving the assets necessary to fulfill the company's obligations to third parties. This conduct not only places the company at risk of insolvency but may also directly lead to its insolvency.[17]

It is noteworthy that German courts are cautious and rarely use the principle of piercing the corporate veil, only in cases where other legal mechanisms fail to ensure justice. This underscores that the principle of limited liability is of key importance in German law and serves the main purpose of a legal entity's existence: protecting its shareholders from the risks of its activities.[18] However, it is worth noting that judicial practice in this regard is not uniform and changes over time.[19]

According to scholarly opinion, applying the doctrine of piercing the corporate veil requires distinguishing between contractual and tort creditors. In the case of contractual creditors, the personal liability of shareholders is not justified, since, when entering into a contractual relationship, the latter can verify the company's financial condition. Tort creditors lack such an opportunity; they cannot choose the debtor, and therefore need more protection.[20]

Based on an examination of available Georgian Judicial practice prior to 2015, two Supreme Court decisions dated May 6, 2015, appear to constitute the first explicit application of the doctrine of piercing the corporate veil. In both decisions, the court identifies indicators that may constitute an abuse of the legal form of the company, namely that the company represents an alter ego of the shareholder, disregard for corporate formalities, and improper capitalization.[21] It should be noted that in Georgian judicial practice, the aforementioned decisions are cited in disputes concerning piercing the corporate veil,[22] and the Supreme Court has not established the shareholder's liability. After the entry into force of the new law, Georgian courts still approach the application of the doctrine of piercing the corporate veil with caution. However, although they have not imposed liability on shareholders, in their assessments, they continue to refer to the same circumstances when determining piercing liability. These include the intentional misrepresentation of creditors; the use of the company as the shareholder's "alter ego"; the commingling

15 Ustiashvili, "Corporate Veil Piercing," 156.

16 Jungmann and Santoro, *German GmbH Law*, 34.

17 Carsten Fløghoff, "Germany," in *European Corporate Law*, eds. Karel Van Hulle and Harald Gesell (Baden-Baden: Nomos, 2006), 159.

18 Jungmann and Santoro, *German GmbH Law*, 33.

19 Müller, *The GmbH*, 93.

20 Burduli et al., *Corporate Law*, 394–95.

21 Decision of the Supreme Court of Georgia of 6 May 2015 No. ას-1307–1245–2014; Decision of the Supreme Court of Georgia of 6 May 2015 No.ას-1158–1104–2014.

22 Decision of the Supreme Court of Georgia of 21 February 2025 No.ას-474–2024; Decision of the Supreme Court of Georgia of 25 April 2024 No. ას-579–2021; Decision of the Supreme Court of Georgia of 13 December 2024 No. ას-1251–2024.

of assets; the disregard of corporate formalities; manifestly inadequate capitalization; and, most importantly, the existence of a direct causal link between the damage and such abuse.[23] It should not be overlooked that the Tbilisi City Court established the piercing of the corporate veil, citing the aforementioned criteria as justification and indicating that the abuse of legal form resulted in the company's insolvency. The court highlighted that the shareholder had deprived the company of assets, thereby preventing it from satisfying its creditors.[24] This demonstrates that Georgian judicial practice maintains the same approach in defining abuse of the legal form of the company, and that the development of judicial practice has not yielded any distinguishing criteria.

3. Abuse of Legal Form

As mentioned, in both Georgian and German law, the use of a company as a facade or alter ego creates a precondition for the abuse of the legal form. German courts consider a company to be used as a facade when it does not perform the function of an independent legal entity and is used solely to pursue the personal interests of its shareholders.[25] It is noteworthy that, as mentioned above, under the alter ego (similar to the facade) doctrine and the interpretation of the Law of Georgia "On Entrepreneurs," the Supreme Court of Georgia established piercing the corporate veil and held the company's shareholder liable for tax obligations. In contrast, the company was unable to fulfill the aforementioned financial obligation towards the creditor, the LEPL Revenue Service of Georgia. Regarding personal liability, the court explained that the above-mentioned doctrine applies in cases of fraud, misrepresentation, and wrongful conduct on the part of a shareholder, when the company is an "instrument" in the hands of the shareholders, an "alter ego" of the shareholder, or a "fiction." In both cases, the court considered tax evasion attempts as a precondition for piercing the corporate veil. It indicated that abuse of the limited liability form by a shareholder occurs when the shareholder is directly involved in the company's management and engages in activities aimed at tax avoidance, that is, when the shareholder uses the company as a vehicle for generating undeclared income.[26]

One should take into consideration that, in terms of confirming the basis for piercing the corporate veil, the disregard of corporate formalities is particularly important. This prerequisite is present when shareholders' meetings are not properly convened and held, when the separation of management and representative powers between shareholders and directors is unclear, when shareholders' and the company's property are confused, and when accounting documentation is not properly maintained. The Supreme Court of Georgia recognized these circumstances in the above-mentioned precedent, in which

[23] Decision of the Supreme Court of Georgia of 19 June 2024, Case No. ას-710–2023; Decision of the Supreme Court of Georgia of 29 February 2024 No. ას-229–2023; Decision of the Supreme Court of Georgia of 13 July 2022 No. ას-532–2021; Decision of the Supreme Court of Georgia of 25 November 2022, Case No. ას-1118–2022.

[24] Decision of Tbilisi City Court of 19 April 2024 No. 2/28903–23.

[25] Jungmann and Santoro, *German GmbH Law*, 33.

[26] Decision of the Supreme Court of Georgia of 6 May 2015 No. ას-1307–1245–2014; Decision of the Supreme Court of Georgia of 6 May 2015 No.ას-1158–1104–2014.

the shareholder was held liable for tax evasion. In that case, the court considered the creation of tax-evasion schemes and the abuse of the limited liability form of the company as a precondition for piercing the corporate veil. The lack of compliance with corporate formalities was manifested in the discrepancy between the documentation confirming the sale of goods.[27]

A good example of breach of corporate formalities is the use of the same addresses, names, and directors by parent and subsidiary companies.[28] According to the German Federal Court, the issue of piercing the corporate veil arises when a shareholder's activities are confused with those of the company; that is, two separate spheres are intertwined.[29] The Federal Supreme Court of Germany in the *Autokran* case indicated that a shareholder may become liable to creditors if their personal assets are commingled with the company's assets in a way that makes it impossible to distinguish between them, thereby making it difficult or impossible to identify the assets against which the company's creditors can seek enforcement.[30] As a general rule, when corporate formalities are observed, authorized capital is paid up (if any), and the company is not formed with the intention of misleading creditors, shareholders are protected from personal liability.[31] The failure to maintain corporate formalities is particularly evident in parent-subsidiary relationships, where the entities may operate under the same address and name and have common management. Such manipulation by the parent company may lead creditors to believe that they are entering into a contractual relationship with the parent company itself, when in fact, the contractual relationship exists with the subsidiary, which is insolvent.[32]

It should be noted that German courts impose personal liability on a shareholder to creditors under the principle of piercing the corporate veil, when the assets of the company and the shareholder are closely intertwined due to non-transparent bookkeeping or other measures.[33] Given that a company and its shareholders are considered separate legal entities, this independence is primarily reflected in the separation of their respective assets. However, a failure to maintain this boundary may mislead creditors and potentially create the precondition for piercing the corporate veil.[34] The German Federal Court emphasizes that piercing the corporate veil is only permissible in extreme cases – when the company is in complete disorganization and obligations cannot be recovered through standard legal means.[35]

---

27 Ibid.
28 Burduli et al., *Corporate Law*, 400.
29 Ibid., 182.
30 Andrea Vicari, *European Company Law* (Berlin: De Gruyter, 2021), 307.
31 Geetika Kaura, "Piercing the Corporate Veil: A Necessary Puncture in the Fabric of the Corporate," *Jus Corpus Law Journal* 3, no. 1 (2022): 665.
32 Burduli et al., *Corporate Law*, 400.
33 Joachim Rosengarten, Frank Burmeister, and Martin Klein, *The German Limited Liability Company*, 9th ed. (München: C.H. Beck, 2020), 48.
34 Burduli et al., *Corporate Law*, 397.
35 Hans S. Birkmose, Mette Neville, and Karsten Engsig Sørensen, *Abuse of Companies* (Alphen aan den Rijn: Kluwer Law International, 2019), 167.

It is worth noting that, when considering the preconditions for piercing the corporate veil, inadequate capitalization is often treated as a circumstance confirming the prerequisite for piercing the corporate veil. Undercapitalization arises when shareholders fail to invest adequately in the business.[36] Furthermore, in the case of improper capitalization, if the company is established in accordance with the law, and the shareholders of the company have done nothing to prevent creditors from seizing and capital maintenance rules are preserved, the shareholder cannot be held liable for the improper financing of the company.[37] The German Federal Court in the *Trihotel* case led to significant changes in German practice, namely, established that a lack of capital alone is not sufficient for personal liability; rather, the fact of the intentional, conscious infliction of damage must be proven.[38] It is essential to distinguish between *bona fide* risk and abuse of the limitation of liability. Unlike in Georgia, German legislation requires the existence of legal capital, which is why insufficient capitalization manifests in two forms: a nominal deficit, when legal capital is not maintained, and a material deficit, when the company's financial resources are disproportionate to its activities.[39] Although German law requires the existence of legal capital, the German Federal Court emphasized that such undercapitalization alone could not give rise to shareholder liability. The court highlighted that shareholders are responsible for providing legal capital, but not for providing financial means for meeting all obligations. Shareholders are obliged only to avoid depriving the company of its assets in any manner incompatible with the rules of capital maintenance.[40] Capital maintenance is a core principle of German company law. This means the obligation to maintain a minimum level of legal capital for joint-stock companies and limited liability companies. Legal capital may be used only to satisfy the company's obligations towards creditors and may not be distributed to shareholders.[41] Additionally, under the principle of capital maintenance, not only are payments to shareholders prohibited, but also payments to third parties in a close relationship with a shareholder. Payments to companies controlled by a shareholder are likewise prohibited. An exemption is the arm's-length principle, under which the company receives, in return, an asset of equal or greater value.[42] Accordingly, undercapitalization, which means not providing financial resources proportional to the company's business activities, must be distinguished from the principle of capital maintenance, which prohibits the distribution of legal capital to shareholders. In Georgia, no minimum legal capital is required for a limited liability company, although companies may freely determine their share capital.[43] This confirms

36 Burduli et al., *Corporate Law*, 398.

37 Cheng Han Tan, Jiangyu Wang, and Christian Hofmann, "Piercing the Corporate Veil: Historical, Theoretical & Comparative Perspectives," *Berkeley Business Law Journal* 16, no. 1 (2019): 179.

38 Müller, *The GmbH*, 94.

39 Iulia Cristina Stroe, "Piercing the Corporate Veil in International Commercial Arbitration: A Brief Overview," *Romanian Arbitration Journal / Revista Romana de Arbitraj* 66, no. 1 (2024): 30.

40 Tan, Wang, and Hofmann, "Piercing the Corporate Veil," 179.

41 Anne Sanders, "Binding Capital to Free Purpose: Steward Ownership in Germany," *European Company and Financial Law Review* 19, no. 4, (2022): 645, https://doi.org/10.1515/ecfr-2022-0020.

42 Andreas Schröder-Frerkes and Anja Göhring, *The Limited Liability Company under German Law (GmbH)* (Woking: German Law Publishers, 2020), 162.

43 Law of Georgia "On Entrepreneurs," Article 134(1).

that inadequate capitalization alone cannot serve as an independent ground for piercing the corporate veil. It is also important to note that personal liability is imposed only on the shareholder responsible for the misuse of the legal form. Other shareholders are not held liable merely by virtue of holding shares in the company. In such cases, piercing the corporate veil applies specifically to one or several shareholders individually.[44]

Based on the above, it seems that Georgian judicial practice regarding piercing the corporate veil is less variable than German judicial practice. However, it is appropriate that both the alter ego theory and the lack of corporate formalities be recognized as manifestations of the abuse of legal form. Given that Georgian law "On Entrepreneurs" does not require legal capital for a limited liability company, nor does it establish in the legal literature an obligation to maintain continuous financing of the company, it is reasonable that only gross undercapitalization is not considered a precondition for piercing the corporate veil. Rather, it can serve as supplementary evidence of abuse of the company's legal form, along with other criteria. Importantly, for the establishment of the first element of piercing the corporate veil – the abuse of legal form – it is necessary that such abuse cause a deterioration of the company's financial situation, rendering it impossible to satisfy the creditors.

4. Inability of the Company to Satisfy the Creditor's Claim as a Precondition

As examined above, the Law of Georgia "On Entrepreneurs" imposes personal liability on a shareholder of a limited liability company if, in addition to the shareholder's abuse of the legal form, the company is unable to satisfy its creditors.[45] Since the aforementioned provision of the law is formulated in such a way as to suggest an "and" connection between the above two circumstances, it is clear that they constitute cumulative preconditions for imposing liability. Moreover, the court should first assess the company's ability to satisfy its creditors, since the issue of piercing the corporate veil arises only when the company is unable to fully or partially satisfy its creditors.[46] Prior to the entry into force of the Law of Georgia "On Entrepreneurs" in 2022, the existing case law interpreted shareholders' liability to creditors as subsidiary liability for the company's obligations. The Supreme Court of Georgia held that shareholders are liable for the company's debts only where they abuse the limited-liability legal form. In other words, if, as a result of such abuse, the creditor is unable to obtain satisfaction directly from the company, the partners may be held personally liable. Thus, according to the instructions of the Supreme Court of Georgia, before examining the prerequisites for personal liability, the insolvency of the debtor must be established. Despite this clarification, the Supreme Court decisions fail to specify the circumstances upon which the determination of debtor insolvency was based.[47] Accordingly, it is reasonable to clarify what constitutes a company's insolvency. The Law

44 Tan, Wang, and Hofmann, "Piercing the Corporate Veil," 180.
45 Law of Georgia "On Entrepreneurs," Article 26(2).
46 Giguashvili and Jugheli, *Commentary on the Law of Georgia on Entrepreneurs*, 62.
47 Decision of the Supreme Court of Georgia of 6 May 2015 No. ას-1307–1245–2014; Decision of the Supreme Court of Georgia of 6 May 2015 No.ას-1158–1104–2014.

on Rehabilitation and Collective Satisfaction of Creditors considers a debtor insolvent if it is unable to cover its due obligations.[48] Thus, in order to determine whether a debtor is insolvent, the debtor's ability to pay its due liabilities must be taken into account, after which the debtor is obliged to disprove the fact of insolvency by proving that its total assets exceed its liabilities.[49] It should not be overlooked that the Law of Georgia "On Entrepreneurs" does not refer to the "insolvent debtor," but rather refers to the inability of the company to satisfy its creditors, which is not equivalent to the insolvency of the company. It is reasonable to assume that the insolvency of the company includes the inability of the company to satisfy its creditors, although the latter may be associated with fewer requirements, for example, registration in the debtor's list of the company for a certain period of time without interruption,[50] or the unsuccessful implementation of enforcement proceedings against the company by creditors.[51] It is also worth noting that the burden of proof of the element of abuse of limited liability lies with the creditor. However, when proving the circumstances of the company's failure to satisfy the creditor, the plaintiff is only obliged to create a preliminary presumption, after which the burden of proof is reversed. The defendant must demonstrate that the company can satisfy the creditors' claims, and there is no need to impose personal liability on the shareholder.[52]

Based on the foregoing analysis, it should be noted, in summary, that the grounds for imposing piercing liability under Article 26(2) of the law of Georgia "On Entrepreneurs" regarding the company's inability to satisfy creditors may not necessarily encompass the company's insolvency solely. The latter shall include fewer requirements, such as prolonged registration in the debtor's registry, unsuccessful enforcement proceedings, and other circumstances.

5. Competition of Remedies

The relationship between piercing the corporate veil and tort liability is very relevant. Recent Georgian judicial practice, rather than the provisions in the Law of Georgia "On Entrepreneurs," applies tort law to impose personal liability on a shareholder.[53] In one case, the founders of a company were found guilty of misappropriating funds from credit union depositors. In the decision, the court noted that one of the founders formally managed the company and that it was at his instigation that the director misappropriated the depositors' funds by granting a loan to a shareholder. The latter did not repay the debt and used it for personal purposes, which is why the company could no longer meet its financial obligations to creditors.[54] As noted above, German courts avoid applying the doctrine of piercing the corporate veil, since shareholders' liability is limited to the company, not

48 Law of Georgia "On Rehabilitation and the Collective Satisfaction of Creditors' Claims," Article 7 (1).

49 Ketevan Meskhishvili et al., *Grounds for Insolvency Proceedings under the Law of Georgia on Rehabilitation and the Collective Satisfaction of Creditors' Claims* (Tbilisi: GIZ, 2021), 29.

50 Burduli et al., *Corporate Law*, 391.

51 Tan, Wang, and Hofmann, "Piercing the Corporate Veil," 177.

52 Giguashvili and Jugheli, *Commentary on the Law of Georgia on Entrepreneurs*, 62.

53 Burduli et al., *Corporate Law*, 401–2.

54 Decision of the Supreme Court of Georgia of 24 December 2020 No. ას-203–2020.

to the creditor. In cases of property misappropriation, German courts rely on piercing the corporate veil, whereas in other cases, they primarily base shareholders' liability on tort law.[55] In addition, according to recent German court practice, the so-called "annihilating interference" by a shareholder constitutes a tortious liability. Such liability arises when a shareholder improperly and against the company's interests uses the company's assets, and this action leads to the company's insolvency or a threat of insolvency.[56] German courts impose liability on shareholders in tort when the shareholder destroys the company's economic basis. This is the case when a shareholder intentionally and knowingly puts the company's economic condition at risk.[57] The shareholder removes the assets from the company in a way that prevents the company from covering its debts. It is worth mentioning that such liability arises only if the company becomes insolvent.[58]

As has already been examined, under German court practice, a shareholder in a limited liability company may be held liable in tort if the shareholder is indifferent to the fact that the company may not be able to meet creditors' claims. In addition, compensation for damages is awarded when a shareholder of an unviable closed corporation continues to conduct business operations through the corporation, despite being aware of the corporation's inability to meet its obligations.[59] This approach was established in 2007 by the German Federal Supreme Court in the Trihotel case, which essentially held that shareholder misconduct that led to a company's insolvency should be treated as damage caused not to creditors, but to the company itself. If a shareholder manipulates the company's assets, he violates the obligation he owes to the company, not to the company's creditors.[60]

According to Georgian law, the distinction between piercing the corporate veil and tort liability is important because each remedy has different preconditions. The preconditions for tort liability, as indicated in the Civil Code of Georgia, are: wrongful act, damage, causal connection between the wrongful act and the damage, and fault of the person who caused the damage. A person will be liable for damages if all four prerequisites are present.[61] The preconditions for piercing the corporate veil are the existence of an abuse of legal form and the company's inability to satisfy its creditors.[62] Although the legal basis for the claim does not change the outcome for the creditor, piercing the corporate veil is more difficult to prove.[63] It is noteworthy that, in the above-mentioned Supreme Court decision, the Revenue Service based its claim on a tort enshrined in the Georgia Civil Code. However, the court indicated that the more specific law of "piercing the corporate

55 Tan, Wang, and Hofmann, "Piercing the Corporate Veil," 183.
56 Ibid., 177.
57 Wirth et al., *Corporate Law in Germany*, 25.
58 Ibid., 24.
59 Vandekerckhove, *Piercing the Corporate Veil*, 62.
60 Stroe, "Piercing the Corporate Veil in International Commercial Arbitration," 31.
61 Decision of the Supreme Court of Georgia of 20 June 2018 No. ას-769–737–2016; Decision of the Supreme Court of Georgia of 4 October 2016 No. ას-176–163–2015; Decision of the Supreme Court of Georgia of 11 April 2019 No. ას-1426–2018.
62 Law of Georgia "On Entrepreneurs," Article 26(2).
63 Burduli et al., *Corporate Law*, 401–2.

veil" should have been applied.[64] It is noteworthy that, in such cases, there is competition between the grounds for the claim between special and general law, which are in an exclusive relationship with each other, and one of the grounds for the claim should be used preferentially due to its special nature.[65] At the same time, according to the Law of Georgia "On Normative Acts," in the event of a conflict between normative acts having equal force, priority shall be given to the normative act adopted later.[66] The same law defines a law of Georgia as a normative act.[67] Both the Civil Code of Georgia and the Georgian law "On Entrepreneurs" constitute laws of Georgia. However, since the Civil Code of Georgia was enacted in 1997,[68] and the law "On Entrepreneurs" entered into force in 2022,[69] the latter-adopted law "On Entrepreneurs" should be given priority.

Given that piercing the corporate veil established by the Law of Georgia "On Entrepreneurs," as previously discussed, is associated with a higher burden of proof, judicial approach regarding bypassing the Law of Georgia "On Entrepreneurs" and more easily imposing liability on the shareholder based on tort, would jeopardize the fundamental essence of a limited liability company – principle of limitation of liability.

6. Conclusion

Based on the research conducted, it is evident that the issue of a shareholder's personal liability arising from piercing the corporate veil encompasses multiple legal aspects. This study reveals that, according to the law of Georgia "On Entrepreneurs," to impose personal liability on a shareholder, it is necessary to prove that the shareholder used the company as an instrument, acting as the company's "alter ego," thereby disregarding the company's separate legal personality. Consequently, in the absence of corporate formalities, the commingling of company and shareholder assets, which leads to the misdirection of creditors, is a specific circumstance that constitutes grounds for holding shareholders personally liable to creditors. As for undercapitalization, it is advisable that this circumstance, similar to the approach of German law, be considered a ground for piercing the corporate veil only in combination with other indicators of abuse of the legal form of limited liability. This approach should be reasonable, as shareholders of a limited liability company under Georgian law are not obliged to contribute the minimum legal capital. The shareholders shall be held liable only if they violate the rules of capital maintenance and unlawfully remove the assets from the company to prevent it from satisfying creditors. It is evident that to establish the first element of veil piercing – abuse of the legal form – it is essential to demonstrate that such abuse led to a deterioration of the company's financial condition, making it impossible for the company to satisfy its creditors.

64 Decision of the Supreme Court of Georgia of 6 May 2015 No. ას-1307–1245–2014.
65 Sophie Chachava, "Competition of Claims and Grounds for Claims in Private Law" (PhD diss., Ivane Javakhishvili Tbilisi State University, 2011), 28.
66 Organic Law of Georgia "On Normative Acts," Article 7(8).
67 Ibid., Article 7(2)(c).
68 Ibid.
69 Law of Georgia "On Entrepreneurs."

It is worth mentioning that under the law of Georgia "On Entrepreneurs," in addition to proving abuse of the legal form by the shareholder, it is also necessary to prove the company's inability to satisfy the creditor's claim to pierce the corporate veil. To establish a company's inability to satisfy the creditors' claim, it is reasonable to consider the following circumstances: initiating insolvency proceedings against the company. However, it should be emphasized that failure to satisfy the creditors does not necessarily mean formal insolvency; this can be demonstrated through less demanding conditions, such as prolonged registration in the debtor's registry, unsuccessful enforcement proceedings, or other circumstances. When proving the company's inability to satisfy creditors, the claimant (creditor) should overcome the initial burden of proof. After this, the burden shifts to the defendant (shareholder) to prove that the company is, in fact, able to satisfy the creditors.

Additionally, as this research revealed, the provision regarding piercing the corporate veil under the Georgia "On Entrepreneurs" law competes with the general tort under the Civil Code of Georgia. In such cases, it is advisable to give precedence to the special and later adopted law "On Entrepreneurs." Another interpretation would jeopardize the fundamental essence of a limited liability company – the principle of limitation of liability.

References

Birkmose, Hans S., Mette Neville, and Karsten Engsig Sørensen. *Abuse of Companies*. Alphen aan den Rijn: Kluwer Law International, 2019.

Burduli, Irakli, Giorgi Makharoblishvili, Ana Tokhadze, Nona Zubitashvili, Giorgi Aladashvili, Gvantsa Maghradze, and Demetre Egnatashvili. *Corporate Law*. Tbilisi: World of Lawyers, 2022.

Chachava, Sophie. "Competition of Claims and Grounds for Claims in Private Law." PhD diss., Ivane Javakhishvili Tbilisi State University, 2011.

Fløghoff, Carsten. "Germany." In *European Corporate Law*, edited by Karel Van Hulle and Harald Gesell, 155–68. Baden-Baden: Nomos, 2006.

Fras, Mariusz. "The Doctrine of Veil-Piercing Liability in Poland and Selected Countries: A Comparative Law Study." *Journal of Civil Law Studies* 14, no. 1 (2022): 101–30.

Giguashvili, Giorgi, and Giorgi Jugheli. *Commentary on the Law of Georgia on Entrepreneurs*. Tbilisi: Investor Council Secretariat, 2022.

Jungmann, Christian, and Daniele Santoro. *German GmbH Law: Das deutsche GmbH-Recht*. 2nd ed. München: C.H. Beck, 2020.

Kaura, Geetika. "Piercing the Corporate Veil: A Necessary Puncture in the Fabric of the Corporate." *Jus Corpus Law Journal* 3, no. 1 (2022): 658–70.

Ketevan, Meskhishvili, Giorgi Batlidze, and Natia Amisulashvili. *Grounds for Insolvency Proceedings under the Law of Georgia on Rehabilitation and the Collective Satisfaction of Creditors' Claims*. Tbilisi: GIZ, 2021.

Müller, Klaus J. *The GmbH: A Guide to the German Limited Liability Company*. 3rd ed. München: C.H. Beck, 2016.

Nelissen Grade, Jean-Marie, and Matthias Wauters. "Reforming Legal Capital: Harmonisation or Fragmentation of Creditor Protection?." In *The European Company Law Action Plan Revisited: Reassessment of the 2003 Priorities of the European Commission*, edited by Koen Geens and Klaus J. Hopt, 25–77. Leuven: Leuven University Press, 2010.

Rosengarten, Joachim, Frank Burmeister, and Martin Klein. *The German Limited Liability Company*. 9th ed. München: C.H. Beck, 2020.

Sanders, Anne. "Binding Capital to Free Purpose: Steward Ownership in Germany." *European Company and Financial Law Review* 19, no. 4 (2022): 622–53. https://doi.org/10.1515/ecfr-2022-0020.

Schröder-Frerkes, Andreas, and Anja Göhring. *The Limited Liability Company under German Law (GmbH)*. Woking: German Law Publishers, 2020.

Stroe, Iulia Cristina. "Piercing the Corporate Veil in International Commercial Arbitration: A Brief Overview." *Romanian Arbitration Journal / Revista Romana de Arbitraj* 66, no. 1 (2024): 17–41.

Tan, Cheng Han, Jasmine Wang, and Christopher Hofmann. "Piercing the Corporate Veil: Historical, Theoretical & Comparative Perspectives." *Berkeley Business Law Journal* 16, no. 1 (2019): 140–204.

Ustiashvili, Giorgi. "Corporate Veil Piercing – In the Doctrine of Georgian, German, and U.S. Law." In *Sergo Jorbenadze 90*, edited by Sergo Jorbenadze, 141–67. Tbilisi: Sulkhan-Saba Orbeliani University, 2019.

Vandekerckhove, Karen. *Piercing the Corporate Veil: A Transnational Approach*. Alphen aan den Rijn: Kluwer Law International, 2007.

Vicari, Andrea. *European Company Law*. Berlin: De Gruyter, 2021.

Wirth, Gerard, Michael Arnold, Ralf Morshäuser, and Steffen Carl. *Corporate Law in Germany*. 4th ed. München: C.H. Beck, 2024.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 53–63
https://doi.org/10.31743/recl.18835
Received: 1 July 2025 | Accepted: 25 February 2026 | Published: 31 March 2026

Implementation of the Principle of Facilitating Exercise of Shareholders' Rights under Polish Law: Critical Remarks

Dominik Mizerski

PhD, Faculty of Law and Administration, University of Silesia in Katowice; correspondence address: ul. Bankowa 11b, 40–007 Katowice, Poland; e-mail: dominik.mizerski@us.edu.pl
https://orcid.org/0000-0002-8253-5038

Abstract: This article analyzes the impact of implementing EU Directive 2017/828 on strengthening shareholder rights and engagement in the Polish legal framework. Despite the directive's aim of facilitating the exercise of shareholder rights, its practical impact has been limited, with only minor improvements observed, such as the obligation for companies to confirm the receipt and registration of votes. The study uses the dogmatic and comparative methods to demonstrate that the legislative changes resulting from the implementation of Directive 2017/828 into Polish law have only marginally improved the legal position of shareholders of listed companies, whose shares are admitted to trading on a regulated market.

Keywords: formal legitimacy, shareholder, public company, general meeting, intermediary, proxy, SRD II

1. Introduction

One aspect of the current discussion about the shape of corporate governance is strengthening shareholders' role in exercising oversight by increasing shareholder engagement. One way to increase this involvement is to adopt instruments that facilitate the exercise of shareholders' rights. The EU legislator adopted this approach through the provisions of Directive 2017/828,[1] the implementation of which was subsequently incorporated into Polish law.

This paper advances the hypothesis that, although the objective of facilitating the exercise of shareholders' rights with a view to enhancing shareholder engagement is clearly articulated at the EU level, the regulatory solutions adopted by the EU legislature and subsequently implemented into Polish law have contributed to this objective only to a limited extent. In particular, it is argued that the practical impact of these provisions on the effective exercise of shareholders' rights appears to be moderate rather than transformative. First, the article demonstrates that the provisions of Polish law implementing Directive 2017/828 do not depart from the literal wording of that legal act, but rather closely replicate its normative content. The analysis indicates that the Polish legislature refrained from introducing autonomous regulatory solutions that would substantially modify or expand upon the standards established at the EU level. Second, the article argues that the transposition of Directive 2017/828 into the Polish legal order largely

[1] Directive (EU) 2017/828 of the European Parliament and of the Council of 17 May 2017 amending Directive 2007/36/EC as regards the encouragement of long-term shareholder engagement (OJ L 132, 20 May 2017), 1–25 (hereinafter: Directive 2017/828).

ISSN 2545-384X (Online)

consisted of clarifying, systematizing, and refining legal instruments already in force before the entry into force of that act. In this respect, the implementation process did not result in a fundamental restructuring of the existing regulatory framework; instead, it primarily served to align pre-existing national provisions with the requirements and terminology of EU law.

The issues covered in this article are essentially limited to considerations arising from the adoption and implementation of Directive 2017/828. The adopted limitations are intended to ensure transparency and substantive precision of the argumentation presented in the paper. The primary research method used to demonstrate the adopted thesis is the legal-dogmatic approach and comparative method. As part of the dogmatic method, the provisions of Directive 2017/828 and the provisions implementing them into the Polish legal system were subjected to a detailed interpretation. This analysis uses linguistic, systemic, and purposive interpretations to assess whether the adopted normative solutions actually achieve the EU legislator's declared objective of strengthening shareholder engagement by facilitating the exercise of shareholders' rights. A comparative method was employed to contrast the content and structure of the norms stipulated in EU legislation with the solutions adopted in the Polish legislature.

2. The Principle of Facilitating the Exercise of Shareholders' Rights in Light of EU Directive 2017/828

As part of the provisions on facilitating the exercise of shareholders' rights, Member States were required to adopt arrangements to ensure that intermediaries assist shareholders in exercising their rights, including the right to attend general meetings and to exercise voting rights at such meetings (Article 3c(1) of Directive 2017/828). The literature rightly emphasizes that the concept of "facilitating the exercise of voting rights" is not limited to the ability to attend and vote at general meetings. It also encompasses a number of other ways in which shareholders can exercise their voting rights.[2] The provisions of Directive 2017/828 establish only minimum requirements, which may be extended by the Member States when implementing the provisions of this legal act into their national legal systems.[3]

In light of the provisions of Directive 2017/828, the Member States may adopt provisions facilitating the exercise of shareholders' rights in the form of ensuring that intermediaries take the necessary steps to enable the shareholder, or a third party designated by that shareholder, to exercise the rights attached to the shares (Article 3c(1)(a) of Directive 2017/828).

The provision of Article 3c(1)(b) of Directive 2017/828 indicates that the exercise of shareholders' rights may also be facilitated through an intermediary exercising the rights attached to the shares under the authority and instructions of and on behalf of the shareholders. In such a case, the intermediary acts as the shareholder's proxy.

---

2 Alessio Bartolacelli, in *The Shareholder Rights Directive II: A Commentary*, eds. Hanne S. Birkmose and Konstantinos Sergakis (Cheltenham: Edward Elgar, 2021), 111.

3 Jan Lieder and Martin Bialluch, in *European Corporate Law: Article-by-Article Commentary*, eds. Peter Kindler and Jan Lieder (Munich–Freiburg: Nomos, 2021), 880.

Furthermore, when voting rights are exercised via electronic communication, Member States are required to ensure that the person casting the vote receives confirmation that the vote was properly received (Article 3c(2), para. 1 of Directive 2017/828). After a general meeting, a shareholder, or a third party designated by the shareholder, should also be able to obtain, at least upon request, confirmation that their votes have been duly registered and counted by the company (Article 3c(2), para. 2 of Directive 2017/828). In addition, it should be noted that the provisions in this area expand those adopted by Directive 2007/36/EC.[4] These provisions required Member States to adopt regulations, in particular, regarding the notice periods for convening general meetings, the content requirements for notices convening such meetings, and measures facilitating the exercise of voting rights (including participation in general meetings by electronic means, voting by proxy, and postal voting).[5]

Additional rules on the transmission of information, the formats to be used, and the deadlines for performing the obligations imposed on intermediaries under the provisions of Directive 2017/828 are set out in Regulation 2018/1212.[6]

3. Implementation of the Principle of Facilitating the Exercise of Shareholders' Rights into Polish Law – General Remarks

The provisions on facilitating the exercise of shareholders' rights, as set out in Article 3c of Directive 2017/828, have been transposed to Polish law in two legal acts: the Act on Trading in Financial Instruments and the Commercial Companies Code.[7] This division not only requires navigating between the provisions of the two acts, but also has consequences, in particular, for the scope of the subjective application of the legal institutions adopted under these acts.

However, as rightly pointed out in the literature, the general principle of facilitating the exercise of shareholders' rights by intermediaries, expressed in Article 3c of Directive 2017/828, has not been implemented directly into Polish law by any statutory amendment.[8] The amendments adopted by the Polish legislature primarily served to clarify

4 Directive 2007/36/EC of the European Parliament and of the Council of 11 July 2007 on the exercise of certain rights of shareholders in listed companies (OJ L 184, 14 July 2007), 17–24 (hereinafter: Directive 2007/36/EC).

5 Lucia Ana Tomić, Marko Žunić, and Suzana Audić Vuletić, "Upcoming Challenges on Regulating Remuneration of the Directors and Implementing Remuneration Policies," *Journal for the International and European Law, Economics and Market Integrations* 5, no. 2 (2018): 328, https://hrcak.srce.hr/213680; Jakub Jan Zięty, *Uprawnienia akcjonariuszy polskich spółek publicznych w świetle Dyrektywy 2007/36/WE* (Warsaw: C.H. Beck, 2015), 65–149; Adam Opalski, "Reforma walnego zgromadzenia spółki akcyjnej – implementacja do prawa polskiego," *Przegląd Prawa Handlowego* 5 (2009): 8–17.

6 Commission Implementing Regulation (EU) 2018/1212 of 3 September 2018 laying down minimum requirements implementing the provisions of Directive 2007/36/EC of the European Parliament and of the Council as regards shareholder identification, the transmission of information and the facilitation of the exercise of shareholders right (OJ L 223, 4 September 2018), 1–18 (hereinafter: Regulation 2018/1212).

7 The Commercial Companies Code of 15 September 2000, Journal of Laws 2024, No. 18, as amended (hereinafter: CCC or Commercial Companies Code).

8 Stanisław Stefaniak, "Rola pośredników tworzących system depozytowy w relacji pomiędzy spółką giełdową a jej akcjonariuszami po implementacji dyrektywy 2017/828," *Przegląd Prawa Handlowego*, no. 2 (2023): 53.

the provisions in force before the implementation of the provisions of Directive 2017/828, or to align the provisions with the instruments adopted under that Directive.

4. Implementation of the Principle of Facilitating the Exercise of Shareholders' Rights in the Provisions of the Act on Trading in Financial Instruments

It should first be pointed out that the provisions of the Act on Trading in Financial Instruments,[9] implementing the provisions of the Directive 2017/828 regarding the principle of facilitating the exercise of rights by shareholders,[10] only apply to companies with their registered office in a Member State, at least one share of which is admitted to trading on a regulated market or on a foreign regulated market (Article 68i(1)(2) of the Act on Trading in Financial Instruments). This is therefore a narrower definition than the concept of a public company under the provisions of the Act on Public Offering,[11] which defines a public company as one with at least one share admitted to trading on a regulated market or introduced to trading in an alternative trading system in the Republic of Poland (Article 4(20) of the Act on Public Offering), as it does not include companies whose shares are introduced to trading in an alternative trading system. This means that the provisions of the Act on Trading in Financial Instruments apply to a relatively small number of companies.

In terms of the provisions of the Act on Trading in Financial Instruments, the Polish legislator imposed additional obligations on intermediaries in the form of providing shareholders with information on the number of shares held at the date of registering their participation at the general meeting (Article 68l(1)(1) of the Act on Trading in Financial Instruments). The intermediary is required to make this information available to the shareholder in accordance with the standardized formats set out in Regulation 2018/1212.[12]

This institution is, in fact, an addition to the legal institutions adopted in Polish law.[13] Indeed, the number of shares is indicated on the registered certificate of the right to participate at the general meeting (Article 406^3 § 1 CCC). In addition, pursuant to Article 406^3 § 2 of the CCC, at the request of the shareholder, pledgee, or usufructuary, all or part of the shares registered in the securities account should be indicated on the certificate. Thus, it seems that the institution provided for in the provision of Article 68l(1)(1) of the Act on Trading in Financial Instruments has little practical use apart from the evidentiary aspect (referred to below).

---

9 Act on Trading in Financial Instruments of 29 July 2005, Journal of Laws 2024, No. 722, as amended (hereinafter: Act on Trading in Financial Instruments).

10 In addition, the definition of a listed company, as regulated in the provisions of the Act on Trading in Financial Instruments, also applies to instruments in terms of shareholder identification and communication between the company and its shareholders.

11 Act on Public Offering and the Conditions Governing the Introduction of Financial Instruments to the Organised Trading System and Public Companies of 29 July 2005, Journal of Laws 2024, No. 623, as amended (hereinafter: Act on Public Offering).

12 Jan Stranz, in *Obrót instrumentami finansowymi. Komentarz*, ed. Tomasz Sójka (Warsaw: Wolters Kluwer, 2022), 426.

13 Stefaniak, "Rola pośredników tworzących system depozytowy," 55.

The provisions of the Act on Trading in Financial Instruments also require intermediaries to provide listed companies with a notice of a shareholder's, or their proxy's, attendance at a general meeting (Article 68l(1)(2) of the Act on Trading in Financial Instruments). However, obtaining such a notice is not a condition for a person to have the formal legitimacy to attend a general meeting.[14] It has been pointed out in the literature that this type of notice may, however, be relevant to shareholders acquiring shares in foreign companies through Polish investment firms, who will want to provide it if the law of the issuer's registered office requires them to participate in a general meeting.[15]

Under the applicable legislation, it should be pointed out that information from intermediaries to shareholders on the number of shares held, or intermediaries sending companies a notice that a shareholder, or their proxy, will attend a general meeting, may be of particular relevance when it is necessary to demonstrate formal legitimacy based on Article 406^3 of the Commercial Companies Code. In this respect, it should be pointed out that there is a dispute in the doctrine.

One view holds that a prerequisite to participating in the meeting is obtaining a registered certificate of right to participate in the general meeting, which is issued at the shareholder's request by the entity maintaining the securities account.[16] This means the shareholder must actively obtain a registered certificate as a prerequisite for the shareholder's legitimacy to participate in the general meeting.

The contrary view is that a sufficient condition for formal legitimacy is that the shares are held in a securities account on the record date.[17] As a result, the shareholder's formal legitimacy can be proved by other evidence.

The author of this paper, who supports this view, points out that, in light of the applicable regulations, such evidence may be the information and documents specified in Article 68l of the Act on Trading in Financial Instruments.[18] Therefore, obtaining a registered certificate of right to participate in the general meeting should not be regarded as a mandatory prerequisite for exercising those rights. Instead, it is one of several legally acceptable methods for proving shareholder legitimacy.

---

14 See: Dominik Mizerski, "O problematyce legitymacji akcjonariusza do udziału w walnym zgromadzeniu spółki publicznej," *Przegląd Prawa Handlowego*, no. 4 (2025): 33–38.

15 Stefaniak, "Rola pośredników tworzących system depozytowy," 54–55.

16 Robert Pabis, in *Kodeks spółek handlowych*, ed. Adam Opalski, vol. 3B, *Spółka akcyjna. Komentarz. Art. 393–490* (Warsaw: C.H. Beck, 2016), 262–63; Andrzej Herbet, in *Kodeks spółek handlowych. Komentarz*, vol. 3, eds. Stanisław Sołtysiński et al. (Warsaw: C.H. Beck, 2013), 1062; Jerzy P. Naworski, in *Kodeks spółek handlowych. Komentarz. Tytuł III. Spółki kapitałowe. Dział II. Spółki Kapitałowe*, eds. Radosław Potrzeszcz and Tomasz Siemiątkowski (Warsaw: LexisNexis, 2012), 777; Michał Bieniak, in *Kodeks spółek handlowych. Komentarz*, Jacek Bieniak et al. (Warsaw: C.H. Beck, 2024), 1267; Judgment of Appellate Court in Kraków of 1 July 2022, I AGa 394/21.

17 Mateusz Rodzynkiewicz, *Kodeks spółek handlowych. Komentarz* (Warsaw: Wolters Kluwer, 2018), 967; Marek Michalski, in *Kodeks spółek handlowych*, ed. Andrzej Kidyba, vol. 3, *Komentarz do art. 301–490* (Warsaw: Wolters Kluwer, 2020), 593–95; Marcin Spyra, in *System Prawa Prywatnego*, ed. Andrzej Szumański, vol. 2b, *Prawo umów handlowych* (Warsaw: C.H. Beck, 2019), 438.

18 Mizerski, "O problematyce legitymacji akcjonariusza," 33–38; in this direction also: Konrad Zacharzewski, in *Prawo rynku kapitałowego*, eds. Marek Wierzbowski, Ludwik Sobolewski, and Paweł Wajda, vol. 1, *Komentarz* (Warsaw: C.H. Beck, 2023), 673.

5. Implementation of the Principle of Facilitating the Exercise of Rights by Shareholders in the Provisions of the Commercial Companies Code

Provisions on sending confirmation to shareholders that their votes have been received and counted by the company have been incorporated into the Commercial Companies Code. In this respect, these provisions supplement and elaborate on the existing provisions of this legal act, which implemented the provisions of Directive 2007/36/EC.[19] This applies, in particular, to the exercise of voting rights by electronic means of communication.

In the case of exercising voting rights through electronic means of communication, the company must immediately send the shareholder electronic confirmation that it has received details of the vote (Article 406^5 § 5 of the Commercial Companies Code). In addition, upon request from the shareholder made within three months from the day of the general meeting, the company has to send the shareholder, or a nominated proxy, confirmation that their vote was properly registered and counted, unless confirmation was already provided to the shareholder, or proxy, earlier (Article 406^5 § 6 CCC).

In the first case, Article 406^5 § 5 of the Commercial Companies Code imposes an obligation on joint-stock companies to send an acknowledgment of receipt of a vote exercised by electronic means. The confirmation referred to in Article 406^5 § 5 of the Commercial Companies Code is mandatory and unconditional, i.e., it does not depend on a request for confirmation submitted by a shareholder or their proxy. Such confirmation should also be sent, regardless of whether the shareholder acted in person or had the right to vote exercised on their behalf by a proxy.

In the second case, as stipulated in Article 406^5 § 6 of the Commercial Companies Code, the company sending the shareholder confirmation that their vote has been correctly registered and counted requires the shareholder to submit a request, which can be sent by any means.[20] In particular, the request may be sent by email, even without an electronic signature or a qualified electronic signature. It appears that the confirmation requirement set forth in Article 406^5 § 6 of the Commercial Companies Code, in accordance with the principle of *lege non distinguente*, applies to the exercise of voting rights at a general meeting and to voting before a general meeting.

The Polish legislator has decided that such a request may be made up to three months after the date of the general meeting. The time limit set out by the Polish legislator is the maximum time limit resulting from Article 3c(2), para. 2 of Directive 2017/828, which allows the introduction of a maximum time limit of three months within which such a request may be submitted. Although the three-month deadline adopted by the Polish legislator is permissible under Directive 2017/828, it appears to be too long. Introducing a shorter deadline, as the German legislator has done, for example, in Section 129(5) of the AktG,[21] which sets a one-month deadline for a shareholder to make a request, would require shareholders to act more quickly to make a request.

---

19 Zięty, *Uprawnienia akcjonariuszy polskich spółek publicznych*, 65–149.

20 Karol Szymański, in *Kodeks spółek handlowych. Komentarz do zmian (tzw. prawo holdingowe)*, eds. Andrzej Szumański, Radosław L. Kwaśnicki, and Filip Ostrowski (Warsaw: C.H. Beck, 2022), 632.

21 The German Stock Corporation Act of 6 September 1965 (Federal Law Gazette I), 1089.

In addition, it should be noted that Article 3c(2) of Directive 2017/828 obliged Member States to impose an obligation on companies to provide shareholders with confirmation that their vote has been duly registered without a separate request from shareholders. However, it seems disproportionate to impose such an additional obligation on companies.

If such confirmations are received by intermediaries, within the meaning of the provision of Article 68i(1)(1) of the Act on Trading in Financial Instruments, the rules on intermediaries sending confirmations (if they act as intermediaries in sending such confirmations) are governed by the provisions of Regulation 2018/1212. The provisions of this legal act set out the detailed timing, formats and content of messages sent by information intermediaries. They also establish the form of the confirmation of receipt and of the correct registration and casting of votes sent by companies.

When assessing the instruments adopted pursuant to Articles 406^5 § 5 and § 6 of the Commercial Companies Code, it is important to note that the provisions implementing the principle of facilitating shareholder rights under the code have a broader scope than those introduced under the Act on Trading in Financial Instruments. The provisions of the Commercial Companies Code, to the extent that they govern the above instruments, apply to any joint-stock or limited joint-stock partnership (shares in such companies do not have to be listed on regulated markets or alternative trading systems for the instruments to apply).[22] In this respect, the subjective scope of these provisions is analogous to that of the provisions adopted in the Commercial Companies Code, which implement Directive 2007/36/EC.[23]

In addition, it should be noted that the rules on intermediaries sending confirmations (if they mediate in connection with such confirmations) are governed by Regulation 2018/1212. The provisions of this legislation set out the detailed timing, formats, and content of the messages transmitted by intermediaries.

While the provision of Article 406^5 § 5 of the Commercial Companies Code obliges companies to immediately forward the confirmation of receipt of votes (the obligation to immediately provide such confirmation also arises from Article 9c(5) first intent of Regulation 2018/1212), the provisions of the Commercial Companies Code do not specify a deadline by when companies have to perform the obligations arising from Article 406^5 § 6 of the Commercial Companies Code. It should be assumed that this obligation takes effect immediately, as with the provision in Article 406^5 § 5 of the Commercial Companies Code. To determine the deadlines for submitting the confirmation specified in Article 406^5 § 6 of the Commercial Companies Code, reference should be made to Article 9c(5) second intent of Regulation 2018/1212, according to which the issuer should confirm the recording and counting of votes promptly, no later than 15 days after

[22] Bieniak, *Kodeks*, 1269; Tomasz Szczurowski, "Nowelizacja kodeksu spółek handlowych w dobie COVID-19," *Przegląd Ustawodawstwa Gospodarczego*, no. 11 (2020): 51, https://doi.org/10.33226/0137-5490.2020.11.6.

[23] Krzysztof Oplustil, "Analiza projektu ustawy implementującej dyrektywę 2007/36/WE w sprawie niektórych praw akcjonariuszy spółek notowanych na rynku regulowanym," *Czasopismo Kwartalne Całego Prawa Handlowego, Upadłościowego oraz Rynku Kapitałowego*, no. 3 (2008): 369.

the request or the general meeting, whichever is later, unless this information is already available.

Notwithstanding the above deadlines for submitting relevant confirmations, it should be noted that a failure by companies to provide confirmations as required under Article 406^5 § 5 and 406^5 § 6 of the Commercial Companies Code is not sanctioned by any specific provision of the code. This does not exclude civil liability for companies' failure to perform these obligations, though such liability is largely theoretical.

Furthermore, a shareholder effectively casts their vote regardless of whether or not the company has sent them confirmation. The confirmation sent by the company should be treated as a statement of fact, i.e., confirmation that the votes have been cast and received, together with possible confirmation that they have been registered and counted. This results from the fact that the provisions of the Commercial Companies Code do not confer any legal effect on such confirmation.

In addition, under the current regulations, it should be noted that a company's failure to issue such a confirmation, both under Article 406^5 § 5 and 406^5 § 6 of the Commercial Companies Code, does not constitute an independent basis for a shareholder to bring an action to annul the given resolution (Article 422 § 1 of the Commercial Companies Code) or an action to declare the invalidity of a resolution (Article 425 of the Commercial Companies Code) of the general meeting. The company's failure to perform the obligations arising under Article 406^5 § 5 or Article 406^5 § 6 does not, in itself, render the resolution inconsistent with any of the conditions specified in Article 422 § 1 and Article 425 CCC. Furthermore, the absence of confirmation does not provide the shareholder with formal grounds to bring an action against the resolution (it is not one of the conditions specified in Article 422 § 2 of the Commercial Companies Code).

Within the scope of regulations aimed at facilitating the exercise of shareholders' rights, the national legislator added the provision in Article 412 § 1^1 of the Commercial Companies Code, which, *expressis verbis*, indicates the possibility of granting an intermediary a power of attorney to exercise voting rights at a general meeting of a public company. This provision applies to public companies within the meaning of the Act on Public Offering, i.e., both to companies whose shares have been admitted to trading on a regulated market and to companies whose shares have been introduced to trading in an alternative trading system.

Article 412 § 1^1 of the Commercial Companies Code[24] implements Article 3c(1)(b) of Directive 2017/828, though its adoption seems to be an example of blind implementation of EU law. Granting a power of attorney to an intermediary would be possible under the provisions of the Commercial Companies Code and the Civil Code, even without an express legal provision. In the literature, it is rightly noted that the regulation's normative value is low.[25] In theory, it only confirms the possibility under the general rules governing the granting of powers of attorney. For this reason, this provision does not create a new rule, but primarily serves a declaratory function.

[24] According to Article 412 §11 of the Commercial Companies Code, the proxy of a shareholder of a public company may be, in particular, an intermediary within the meaning of the Act on Trading in Financial Instruments.

[25] Michalski, *Kodeks*, 652.

Regarding the power of attorney granted to intermediaries under Article 412 § 1^1 of the Commercial Companies Code, the general rules on granting powers of attorney by shareholders of public companies apply. In particular, Article 412^1 of the Commercial Companies Code provides that a power of attorney to represent a shareholder at a general meeting of a public company may be granted either in writing or electronically, with no requirement that it be in electronic form or that it be accompanied by a qualified electronic signature to be effective.

6. Conclusions

Although the EU legislator clearly indicated the need to strengthen shareholder engagement by facilitating the exercise of their rights, the paper's conclusions confirm that the solutions adopted in Directive 2017/828 and subsequently incorporated into the Polish legal system achieve this goal only to a limited extent. Furthermore, the Polish provisions implementing Directive 2017/828 adhere closely to the wording of that legal act and do not deviate from its literal content. Such transposition did not lead to a fundamental overhaul of national regulations, but rather resulted in their clarification and terminological adjustment. Consequently, the impact of the new regulations on increasing shareholder activity is moderate,[26] and while the adopted instruments formally strengthen the ownership position, they are not fundamentally transformative.

In my opinion, the most significant area of strengthening the shareholder's position concerns the introduction of an obligation on companies to send a confirmation of receipt of a vote (Article 406^5 § 5 of Commercial Companies Code), and an obligation to send a confirmation that the shareholder's vote has been correctly registered and counted (Article 406^5 § 6 of the Commercial Companies Code). The introduction of these institutions is all the more important in light of the fact that public companies have increasingly enabled their shareholders to exercise their voting rights through electronic means of communication.[27] This also applies to public companies, whose shares were admitted to trading on a regulated market. In 2019, in a sample of 95 companies with their registered offices in Poland whose shares were admitted to trading on the regulated market of the Warsaw Stock Exchange between January 1, 2014 and December 31, 2023, and which were included in the WIG20,[28] mWIG40,[29] and sWIG80[30] indices as at June 30, 2024, only

[26] See more on potential impact of adoption of the Directive 2017/828 on the shareholder engagement in Poland: Dominik Mizerski, "Evaluating Long-Term Shareholder Engagement Instruments under Directive 2017/828," in *Právo, Obchod, Ekonomika XIV. Zborník Vedeckých Prác. Výber z vedeckých príspevkov*, eds. Ján Husár and Regina Hučková (Kosice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2025), 36–45.

[27] Nevertheless, it seems that this change is more a result of measures introduced in response to the COVID-19 pandemic than of the companies' own decisions – see more on changes in law adopted after spread of COVID-19 pandemic: Piotr Pinior, "Impact of the COVID-19 Pandemic on Company Law. Shareholders' Meetings and Resolutions," *European Company and Financial Law Review* 19, no. 1 (2022): 100–27, http://dx.doi.org/10.1515/ecfr-2022-0004.

[28] Stock market index of the 20 largest companies listed on the Warsaw Stock Exchange.

[29] Stock market index of the 40 largest companies not including the 20 companies included in the WIG20 index.

[30] Stock market index of the 80 largest companies, after the companies included in the WIG20 and mWIG40 indices.

two companies enabled participation in the annual general meetings held that year by means of electronic communication and the exercise of voting rights in this way. In 2020, 21 companies enabled shareholders to do so; in 2021, 27; in 2022 and 2023, 26.

Other amendments, enacted as a result of implementing the provisions of Directive 2017/828, in respect of facilitating the exercise of shareholders' rights in the Polish legal order, are of marginal significance for shareholders under Polish law. This applies, in particular, to the introduction of Article 412 § 1^1 of the Commercial Companies Code, which *expressis verbis* permits the granting of powers of attorney to intermediaries. The introduction of this express authorization was unnecessary because, as indicated in this paper, granting powers of attorney to such entities was permissible under general rules even before the provisions of Directive 2017/828 came into effect.

On the other hand, as regards the provisions of the Act on Trading in Financial Instruments, the adoption of the institutions provided for in Article 68l of the Act on Trading in Financial Instruments, i.e., providing shareholders with information on the number of shares they hold at the time of registering to attend the general meeting and providing a notice to the stock exchange company that the shareholder or their proxy are participating at the general meeting, may be seen as a supplement to the regulations in force, in particular with regard to the principles of determining the list of entities entitled to participate at general meetings. The key determinant of legitimacy to participate in a general meeting remains the holding of shares on the record date. At the same time, the documentation transmitted pursuant to Article 68l of the Act on Trading in Financial Instruments merely facilitates the demonstration of this fact in cases of procedural doubt. Thus, the new solutions refine and complement the existing system without modifying its conceptual foundations.

Moreover, the scope of application of these instruments remains significantly limited due to the narrow subjective reach of the Act on Trading in Financial Instruments. Since its provisions apply exclusively to companies with at least one share admitted to trading on a regulated market, they affect only a fraction of entities commonly understood as public companies under Polish law. In this regard, it would be advisable to extend the application of these provisions also to companies whose shares are admitted to trading on an alternative trading system.

Funding: This research was fully funded by the National Science Centre, Poland; project number: 2024/53/N/HS5/00255.

References

Bartolacelli, Alessio. "Article 3c–3f: Facilitation of the Exercise of Shareholder Rights." In *The Shareholder Rights Directive II: A Commentary*, edited by Hanne S. Birkmose and Konstantinos Sergakis, 104–42. Cheltenham: Edward Elgar, 2021.

Bieniak, Michał. In *Kodeks spółek handlowych. Komentarz*, edited by Jacek Bieniak et al., 1267, 1269. Warsaw: C.H. Beck, 2024.

Herbet, Andrzej. In *Kodeks spółek handlowych. Komentarz*, vol. 3, edited by Stanisław Sołtysiński, Andrzej Szajkowski, Andrzej Szumański, and Janusz Szwaja, 1062. Warsaw: C.H. Beck, 2013.

Lieder, Jan and Martin Bialluch. In *European Corporate Law: Article-by-Article Commentary*, edited by Peter Kindler and Jan Lieder, 880. Munich–Freiburg: Nomos, 2021.

Michalski, Marek. In *Kodeks spółek handlowych*. Vol. 3, *Komentarz do art. 301–490*, edited by Andrzej Kidyba, 593–95, 652.Warsaw: Wolters Kluwer, 2020.

Mizerski, Dominik. "Evaluating Long-Term Shareholder Engagement Instruments under Directive 2017/828." In *Právo, Obchod, Ekonomika XIV. Zborník Vedeckých Prác. Výber z vedeckých príspevkov*, edited by Ján Husár and Regina Hučková, 36–45. Kosice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2025.

Mizerski, Dominik. "O problematyce legitymacji akcjonariusza do udziału w walnym zgromadzeniu spółki publicznej." *Przegląd Prawa Handlowego*, no. 4 (2025): 33–38.

Naworski, Jerzy P. In *Kodeks spółek handlowych. Komentarz. Tytuł III. Spółki kapitałowe. Dział II. Spółki Kapitałowe*, edited by Radosław Potrzeszcz and Tomasz Siemiątkowski, 777. Warsaw: LexisNexis, 2012.

Opalski, Adam. "Reforma walnego zgromadzenia spółki akcyjnej – implementacja do prawa polskiego doktryny 2007/36/WE." *Przegląd Prawa Handlowego* 5 (2009): 8–17.

Oplustil, Krzysztof. "Analiza projektu ustawy implementującej dyrektywę 2007/36/WE w sprawie niektórych praw akcjonariuszy spółek notowanych na rynku regulowanym." *Czasopismo Kwartalne Całego Prawa Handlowego, Upadłościowego oraz Rynku Kapitałowego*, no. 3 (2008): 365–98.

Pabis, Robert. In *Kodeks spółek handlowych*. Vol. 3B, *Spółka akcyjna. Komentarz. Art. 393–490*, edited by Adam Opalski, 262–63.Warsaw: C.H. Beck, 2016.

Pinior, Piotr. "Impact of the COVID-19 Pandemic on Company Law. Shareholders' Meetings and Resolutions." *European Company and Financial Law Review* 19, no. 1 (2022): 100–27. http://dx.doi.org/10.1515/ecfr-2022-0004.

Rodzynkiewicz, Mateusz. *Kodeks spółek handlowych. Komentarz*. Warsaw: Wolters Kluwer, 2018.

Spyra, Marcin. In *System Prawa Prywatnego*. Vol. 2b, *Prawo umów handlowych*, edited by Andrzej Szumański, 438. Warsaw: C.H. Beck, 2019.

Stefaniak, Stanisław. "Rola pośredników tworzących system depozytowy w relacji pomiędzy spółką giełdową a jej akcjonariuszami po implementacji dyrektywy 2017/828." *Przegląd Prawa Handlowego*, no. 2 (2023): 43–58.

Stranz, Jan. In *Obrót instrumentami finansowymi. Komentarz*, edited by Tomasz Sójka, 426. Warsaw: Wolters Kluwer, 2022.

Szczurowski, Tomasz. "Nowelizacja kodeksu spółek handlowych w dobie COVID-19." *Przegląd Ustawodawstwa Gospodarczego*, no. 11 (2020): 46–52. https://doi.org/10.33226/0137-5490.2020.11.6.

Szymański, Karol. In *Kodeks spółek handlowych. Komentarz do zmian (tzw. prawo holdingowe*), edited by Andrzej Szumański, Radosław L. Kwaśnicki, and Filip Ostrowski, 632. Warsaw: C.H. Beck, 2022.

Tomić, Lucia Ana, Marko Žunić, and Suzana Audić Vuletić. "Upcoming Challenges on Regulating Remuneration of the Directors and Implementing Remuneration Policies." *Journal for the International and European Law, Economics and Market Integrations* 5, no. 2 (2018): 323–44. https://hrcak.srce.hr/213680.

Zacharzewski, Konrad. In *Prawo rynku kapitałowego*. Vol. 1, *Komentarz*, edited by Marek Wierzbowski, Ludwik Sobolewski, and Paweł Wajda, 673. Warsaw: C.H. Beck, 2023.

Zięty, Jakub Jan. *Uprawnienia akcjonariuszy polskich spółek publicznych w świetle Dyrektywy 2007/36/WE*. Warsaw: C.H. Beck, 2015.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 65–85
https://doi.org/10.31743/recl.18965
Received: 14 August 2025 | Accepted: 22 February 2026 | Published: 31 March 2026

Homework in the Countries of the Visegrad Group (V4): A Comparative Legal Study

Michał Barański

PhD, Assistant Professor, Faculty of Law and Administration, University of Silesia in Katowice, correspondence address: ul. Bankowa 11b, 40–007 Katowice, Poland; e-mail: michal.baranski@us.edu.pl
https://orcid.org/0000-0001-6797-8124

Norbert Richter-Sitko

MA, PhD Student, Deák Ferenc Doctoral School of Law, University of Miskolc, Hungary, Junior Researcher, Central European Academy of the University of Miskolc, Budapest, Hungary, correspondence address: st. Városmajor 12–14, "Major Udvar" building, HU-1122 Budapest, Hungary; e-mail: norbert.j.richter.sitko@gmail.com
https://orcid.org/0000-0001-8674-3267

Abstract: Derived from the traditional cottage industry, homework has played a significant social and economic role in Europe for centuries. In the digital economy era, homework is acquiring new significance, particularly in the context of flexible forms of work, such as remote working or home-based platform work. This article focuses on the Visegrad Group countries, analyzing the regulation of homework within each country's national legal system. This analysis will help determine the status of homework within labor law and its legal position. To this end, the authors employed a historical approach to examine the evolution of homework, a dogmatic approach to establish its legal standing in relation to the employment relationship and contract, and a comparative approach to identify convergences in national regulations. The final result of the comparative study reveals the diversity of homework regulations within the Visegrad Group. These range from a shift towards remote work (Czech Republic), through to separate yet compatible regulations on telework and homework within the employment relationship (Slovakia and Hungary), to the distinction between remote work and homework (Poland).

Keywords: homework, Visegrad group countries, comparative legal analysis, remote work, labor law

1. Introduction

Homework, derived from the traditionally understood cottage industry, has played a significant social and economic role in Europe for centuries. It enabled individuals who, for various reasons, could not take up employment in industrial establishments to earn an income, such as those caring for family members or artisans working from home (typically in rural areas). During industrialization, homework served as an important transitional element between agricultural labor and the factory system. Today, in the era of the digital economy, homework is assuming new significance, particularly in the context of flexible forms of work (e.g., remote work). Homework, teleworking, and home-based platform work have a particular common feature. They are all types of work that are not tied to the employer's workplace but can be done anywhere, most often at the employee's home or in coworking facilities. Essentially, the distinction between homework and teleworking was the use of information and communication technologies and where work, which

ISSN 2545-384X (Online)

could also be performed at the employer's premises, is carried out away from those premises regularly.[1] Home-based platform work operates through digital labor platforms that connect service providers with potential customers. Additionally, work performance is mainly task-based ("gig economy") and coordinated by algorithms rather than traditional management.[2]

Due to the lack of uniform national regulations and terminological differences already apparent at the conceptual level, and to avoid creating an artificial definition for this study, the comparative legal analysis conducted herein refers to the definition of homework laid down in Article 1(a) of the International Labour Organisation (hereinafter: ILO) Convention No. 177 on Home Work.[3] According to the text of that Convention, the term "homework" means

> work carried out by a person, to be referred to as a homeworker, (i) in his or her home or in other premises of his or her choice, other than the workplace of the employer; (ii) for remuneration; (iii) which results in a product or service as specified by the employer, irrespective of who provides the equipment, materials or other inputs used, unless this person has the degree of autonomy and of economic independence necessary to be considered an independent worker under national laws, regulations or court decisions.

In many European countries, the legal nature of homework has raised serious doubts for years, necessitating an analysis of existing regulations across different legal systems. Above all, classifying the homework contract within the labor law regime proves problematic – particularly in determining the extent to which labor law provisions may apply to homework.[4]

The primary objective of this study is to answer the question of whether, in the countries of the Visegrad Group (V4), homework constitutes merely a social fact or whether it functions within the respective legal system as a distinct legal category (and if so, whether this category falls within the labor law regime). Answering this fundamental question allows for a detailed comparative legal analysis in the following areas: (1) the possibility of identifying features of the national employment relationship in the context of homework (e.g., the personal performance of work or a level of subordination at least resembling that found in employment relationships); (2) whether the legal basis of homework is a best-effort contract or a result-based contract; and (3) the role of homework as a means of femininizing work performance (e.g., within the framework of the flexicurity employment model).[5] It must be emphasised that the legal regime alone does not definitively

---

1 Compare with ETUC, UNICE/UEAPME, and CEEP, *Framework Agreement on Telework* (Brussels, 16 July 2002).

2 Cf. Steven Vallas and Juliet B. Schor, "What Do Platforms Do? Understanding the Gig Economy," *Annual Review of Sociology* 46, no. 1 (2020): 273–94, https://doi.org/10.1146/annurev-soc-121919-054857.

3 International Labour Organization, *Home Work Convention, 1996 (No. 177)* (Geneva, 1996). It should be noted that none of the V4 countries has yet ratified the Convention and is therefore not obliged to comply with its provisions.

4 Teresa Wyka, "Sytuacja prawna osób wykonujących pracę nakładczą," *Acta Universitatis Lodziensis. Folia Iuridica* 25 (1986): 5 and the literature cited therein.

5 Flexicurity can be defined as "an integrated strategy to enhance, at the same time, flexibility and security in the labour market." See also: European Commission, *Towards Common Principles of Flexicurity: More and Better Jobs through Flexibility and Security*, COM(2007) 359 final (Brussels, 2007). Flexicurity is a concept

determine the legal nature of a given contract. In conclusion, resolving the aforementioned issues – i.e., determining the legal nature of homework in each V4 country – at the national level will allow for an assessment of whether a homeworker is, or should be, considered an employee.

The choice to analyze the Visegrad Group countries in this comparative legal study, aside from limits imposed by the scope of such a work, stems from several important factors. Firstly, these countries share a similar history of systemic transformation, which has shaped the development of their legal systems – including regulations concerning atypical forms of work. Secondly, all V4 countries are members of the European Union, which requires them to implement EU labor law. The absence of a unified concept of homework under EU law makes the analysis of national solutions particularly relevant. Thirdly, the observed diversity of approaches within the V4 provides an opportunity to better evaluate the effectiveness of existing regulations. Studying the V4 legal systems may also help identify directions for future reforms, especially given the growing importance of flexible forms of work (e.g., remote work) and new EU labor law regulations (e.g., concerning home-based platform work).

2. Legal Regime of Homework in Visegrad Group Countries (V4)

2.1. Legal Regime of Homework in Czechia

To lay the basis for the homework in the Czech and Slovak labor law system, it is necessary to consider the first regulation introduced to the newly formed Czechoslovak state – the Act on the Regulation of Labour and Wage Conditions of Homework.[6] Section 2(a) of the Act defined homeworkers as "persons engaged in the production or processing of goods away from the premises of their employers, generally in their own homes, and do not carry on trades under the trade regulations."[7] After the end of the Second World War and with the changes in the economic system underway, there was a tendency to gradually reduce homework due to work safety concerns and the impossibility of ensuring sufficient control over work performance.[8] Also worth mentioning is the ruling of the Supreme Court of Czechoslovakia from July 4, 1959[9] (before the definition of homeworker was

that has to be defined as part of an ongoing process. It should not be a standardized model that can be applied in the same way, for example, across all European Union Member States. Cf. Michał Barański, "Employment Flexibility in Times of Crisis," *Studia Iuridica*, no. 95 (2023): 12, https://doi.org/10.31338/2544-3135.si.2022-95.1; it should be emphasized that the meaning of the flexicurity concept has evolved in response to changing economic, technological, and social conditions. See also: European Commission, *Establishing a European Pillar of Social Rights*, COM(2017) 250 final (Brussels, 2017).

6 Act on the regulation of working and wage conditions for domestic work of 12 December 1919, No. 29/1920 Coll.

7 Cf. Jan Pichrt, "Několik Poznámek k Pracovním Vztahům Domovníků, Obchodních Pomocníků a Domáckých Zaměstnanců v Období První Republiky," in *Caro Amico: 60 Kapitol pro Michala Skřejpka Aneb Římské Právo Napříč Staletími*, eds. Petr Bělovský and Kamila Stloukalová (Praha: Auditorium, 2017), 312–23.

8 Martin Štefko, "§ 317," in *Zákoník Práce. Komentář*, eds. Miroslav Bělina and Ljubomír Drápal (Praha: C.H. Beck, 2019), 1254–56.

9 Own translation, Decision of Czechoslovak Supreme Court of 4 June 1959, Cz 176/59.

introduced in the labor code in 1965)[10] that consider on the legal nature of homework. It stated that:

> It is not possible to reach the conclusion that a contract under which a particular employee undertakes to perform specific work, or to perform specific work at home, is always a contract of employment, if a number of differences can be identified compared with a contract of employment. (...) It follows from the above that neither by the nature and content of the arrangement, the subject of which is the work performed by the employee concerned at home, nor by the applicable statutory provisions, can the conclusion be reached that work performed at home will always be the subject of an employment contract.

Nonetheless, with the new labor code of 1965, Czechoslovak lawmakers introduced an atypical form of work, i.e., work performed outside the employer's premises. According to Article 267(2) the homework, understood as the work of

> employees (so-called "homeworkers," Czech: *domáčtí zaměstnanci*) who do not work at the employer's workplaces but, according to the terms and conditions agreed in the employment contract, perform agreed work for the employer at home during their own working hours was governed by the labor code.

However, these regulations diminished certain employee rights, including those concerning fixed weekly working time, downtime compensation, overtime pay, and holiday pay. The government also retained the power to introduce further derogations for homeworkers via regulation, or to grant compensation for significant personal work hindrances, should their unique working conditions necessitate such adjustments.

Along with the transition to a new economic system and the dissolution of Czechoslovakia in 1991, newly established countries introduced new labor codes that again sought to regulate homework, with particular changes driven by technological development. From this point on, we will focus on the Czech regulation on homeworking. The section on the Slovakian regulation is addressed in the following subchapter.

With the new Czech Labour Code (Czech: *Zákoník práce*, hereinafter: CZP), introduced in 2006,[11] the legislator has regulated work performed outside the employer's premises in Article 317. Despite the explanation to the new CZP stating that the new regulation implements new forms of employments,[12] but employment differently, in reality, it is a closely similar regulation adapted to the new economic and technological

[10] Act on Labor Code of 30 June 1965, 65/1965 Sb.

[11] Act on Labor Code of 7 June 2006, 262/2006 Sb.

[12] Explanatory memorandum to Act No. 262/2006 Coll., Labour Code, p. 40, accessed May 20, 2025, https://vlada.gov.cz/assets/urad-vlady/poskytovani-informaci/poskytnute-informace-na-zadost/Priloha_3_Duvodova_zprava.pdf.

(telework) environment.[13] Nonetheless, the legislator did not follow the telework criteria set out in the Framework agreement on telework.[14]

In October 2023, Article 317 was changed completely. After the amendment, the article in simplified version states that the "performance of remote work (Czech: *práce na dálku*) is only possible based on a written agreement between the employer and the employee," without specifying the content of the agreement.[15] Paragraph 2 of Article 317 sets out a relative dispositive norm granting the parties greater autonomy in terminating the remote work agreement. In similar matters as the previous regulation, para. 4 changed for the employees whose working time is scheduled by themselves, the scope of application of provisions regarding the scheduling of working hours, downtime or interruptions of work due to inclement weather shall apply; compensation for wages or salary, in the event of other important personal obstacles to work. However, with effect from January 1, 2025, para. 4 of Article 317 was repealed, and for remote work, the general provision of Article 87a (scheduling of working time by the employee) was found in force.[16]

2.2. Legal Regime of Homework in Slovakia

Article 52 of the Slovak Labour Code (Slovak: *Zákonník práce*,[17] hereinafter: SZP) regulates homework and telework (Slovak: *Domácka práca a telepráca*) as a single provision. The current provision is a result of COVID-19, which has led to an amendment of the Labour Code in 2021,[18] making it more flexible by allowing employees to organize their own working time.[19]

Homework is understood as work that can be performed at the employer's workplace and is performed regularly within the scope of the prescribed weekly working time, or part of it, from the employee's home. However, the legislator broadened the definition of employee's house to "the agreed place of work outside the employer's place

---

13 According to Article 317 of the CZP, this Act covers employees who work remotely and set their own hours and conditions, provided they are not subject to regulations regarding work scheduling, downtime or weather-related interruptions. Furthermore, unless implementing legislation specifies otherwise, such employees are not entitled to compensation for wages during personal work obstacles, overtime pay/time off, or extra pay for public holiday work; see also: Eva Dandová, "Práce na dálku," *BHP. – Bezpečnost a Hygiena Práce*, no. 7/8 (2025): 14–77.

14 Cf. European Commission, *Report on the Implementation of the European Social Partners' Framework Agreement on Telework*, SEC(2008) 2178, accompanying COM(2008) 412 final (Brussels, 2008), accessed May 20, 2025, https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52008sc2178.

15 Previous draft proposals recommended that remote working agreements should detail how employers assign tasks, monitor performance and ensure health and safety in the workplace, cf. Aneta Giedrewicz-Niewińska, Viktor Križan, and Jana Komendová, "The Obligations of the Employer in the Implementation of Remote Work: The Examples of Slovakia, the Czech Republic and Poland," *Białostockie Studia Prawnicze* 29, no. 2 (2024): 89, https://doi.org/10.15290/bsp.2024.29.02.07.

16 Margerita Vysokajová, "§ 317," in *Zákoník práce: komentář*, eds. Petr Hůrka et al. (Praha: Wolters Kluwer, 2025): 731–35.

17 Act on Labor Code of 8 August 2001 č. 311/2001 Z. z.

18 Act on amending Act No. 311/2001 Coll. Labor Code, as amended, and amending certain acts of 4 February 2021.

19 Helena Barancová, "Nová právna úprava domáckej práce a telepráce," *Právny Obzor* 105, no. 1 (2022): 3, https://doi.org/10.31577/pravnyobzor.2022.1.01.

of work" (Article 52(3) SZP). Telework differs from homework in that it requires additional conditions to perform the work using information technology and to transmit electronic data regularly at a distance.[20] The performance of homeworking or teleworking shall require the agreement of the employer with the employee in the employment contract. Parties were granted higher scope of the autonomy regarding the agreement on performing homework or telework, which extend to exclusivity of performing work in whole or in part whole or in part at a place designated by the employee, if the nature of the work so permit (Article 52(5) SZP), compliance with scheduled working time or flexibility of working hours (Article 52(6) SZP).[21] Slovak regulations also oblige the employer to provide work tools (as a rule) and data protection (Article 52(8) SZP). Moreover, employees performing homework or telework shall have the "right to disconnect,"[22] and the "employer shall not treat as a failure to perform an obligation if an employee refuses to perform work or comply with an instruction at that time" (Article 52(9) SZP). Significantly, Article 52(2) SZP excluded from the scope of the homework or telework occasional "home office."[23]

2.3. Legal Regime of Homework in Hungary

The first attempt to regulate homework (Hungarian: *A bedolgozói munkaviszony*) in the Hungarian legal system was introduced in 1967,[24] and amended in 1981[25] by the ministerial Decrees on homework. The homeworker in both Decrees may be any natural person who independently performs physical or non-physical (so-called "intellectual") work for which the performance requirement can be specified as a work standard or other quantitative or qualitative indicators. The workplace of the homeworker was outside the employer's premises, typically the homeworker's house. Remuneration is linked to the rates of full-time employees for similar work, and the parties are obliged to determine pay at the time of assignment. The material liability of the homeworker for the resources assigned to him, except when the damage is due to unrelated causes, refers to the general principles of labor law. Both Decrees provide mechanisms for reimbursing costs incurred by the homeworker in connection with the work performed. Finally, the employer retains his right to control the work performed and to give instructions regarding the materials entrusted.

---

20 Iveta Matlovičová, "Pravidelná a príležitostná práca z domácnosti zamestnanca," *Dane a Účtovníctvo v Praxi* 26, no. 5 (2021): 47–48.

21 However, according to Article 52(7) SZP, if the employee determines his own working time, his employment is subject to the exceptions to the working time and the related rights to remuneration, cf. Zuzana Homer, "Výkon domácej práce a telepráce v kontexte aktuálnej aplikačnej praxe," in *Zamestnanec v digitálnom prostredí*, eds. Monika Minčičová, Marcel Dolobáč, and Jana Žuľová (Košice: Univerzita Pavla Jozefa Šafárika, 2021), 120–21.

22 Unless on-call or overtime work is ordered or agreed with him at that time, during the taking of leave, on a holiday for which the work has fallen away, and during a hindrance to work.

23 Para. 8(b) and paras. 9 to 11 shall apply *mutatis mutandis* to this type of work, cf. Jozef Toman, "§ 52. Domácka práca a telepráca," in *Zákonník práce, Zákon o kolektívnom vyjednávaní – Komentár*, 5th ed., eds. Marek Švec and Jozef Toman (Bratislava: Wolters Kluwer 2023), points 10–11.

24 Decree No. 16/1967 (XII. 27.) on the employment of home workers.

25 Decree No. 10/1981 (IX. 29.) on the employment of home workers.

In the aftermath of the economic system's transformation, a new Decree on homework relationship was promulgated in 1994,[26] with effect until 2012, which was then incorporated into the Labour Code (Hungarian: *a munka törvénykönyvéről*, hereinafter: Mt.) from 2012.[27] The major change with the incorporation of this regulation was the removal of the possibility for the homeworker to use the work of assistants (in this case, family members). Additionally, the employer has no right to give the employee instructions that exceed the techniques used and the way of working. The homework employment relationship is set out in chapter XV of the Mt., which comprises the special provisions relating to employment relationships by type.[28]

Section 198–200 Mt. considers the homework as a work that can be performed independently and for which remuneration is based solely on the work performed. An employee's work performance is remunerated on a performance-based wage under Section 137(2) Mt. Additionally, Section 199 regulates the reimbursement of employee expenses and the payment of remuneration. The parties can decide on the homeworker's workplace, but it need not be the homeworker's home. The employer's right of control/instruction, unless otherwise agreed, is limited to the specification of the technique and work processes to be used by the employee. The Mt. states that, as a rule, the employee shall carry out the work using his own means, and his working arrangements should not be fixed. The employment contract shall, at least, define the work performed by the employee, the place where work is carried out and the method and extent of covering expenses. Section 200(2) Mt. stipulates that, in the event of performance that does not align with the negotiated requirements and is attributable to the employee, no remuneration or reimbursement of expenses should be granted. However, if the employer may use all or part of the results of the work, the employer shall pay reduced remuneration and reimburse expenses.

Telework, as the second category that allows employees to perform work outside the traditional workplace, is regulated by Section 196 Mt. Currently, telework means "where the employee works at a place other than the employer's facilities in some or all of the working time."

2.4. Legal Regime of Homework in Poland

Historically, Polish legislation initially employed exclusively the term "homework" (Polish: *praca nakładcza* / *praca chałupnicza*) in generally applicable legal acts. The first definitions of *praca chałupnicza* (cottage work) raised many doubts in distinguishing a cottage worker (Polish: *chałupnik*) from a craftsman or a laborer.[29] It was not until the 1937 Regulation of the Minister of Industry and Trade that cottage work, which had been excluded from the scope of industrial law, was defined as gainful employment and listed

[26] Government Decree No. 24/1994 (II.25.) on the employment of home workers.

[27] Act on the Labour Code of 13 December 2011, 2012. évi I.

[28] That chapter regulates, for instance, fixed-term employment relationships, call for work, job sharing, employee sharing, teleworking, and the situation of incapacitated employees, etc.

[29] Teresa Wyka, "Społeczno-ekonomiczne przesłanki rozwoju nakładztwa w Polsce," *Z Problematyki Prawa Pracy i Polityki Socjalnej*, no. 3 (1980): 172.

alongside folk and domestic industry.[30] In that regulation, cottage work was precisely defined as:

> professional and gainful employment of natural persons, performed in the worker's own dwelling or in another place where the working regime is not imposed by the principal, consisting in the production, processing or finishing of any type of goods, based on a contract concluded with the principal, on his order and at his expense – provided that the work is carried out independently or solely with the assistance of family members and cohabitants.[31]

Nevertheless, in practice, cottage industry in the interwar period encompassed such a wide variety of forms that it was often difficult to determine whether it should be classified as independent craftsmanship, folk industry, or domestic production.[32]

Immediately after World War II, homework continued – at least at the regulatory level – to be recognized as a form of production alongside domestic industry, folk industry, and craftsmanship, and was excluded from the scope of industrial law. At that time, homework was defined as

> gainful work performed by natural persons, on commission and at the expense of entities in the socialized economy (principals), consisting of: (1) the production of goods, items, or their parts from materials supplied by the principal; (2) the finishing, refining, repair, and maintenance of goods, items, or their parts, as well as the provision of other services.[33]

The term "homework contract" (Polish: *umowa o pracę nakładczą*) first appeared by name in the Polish Labor Code (Polish: *Kodeks pracy*, hereinafter: KP),[34] which, despite numerous amendments, remains in force to this day. Only upon the Labor Code's entry into force (on January 1, 1975) did "the homework contract cease to be merely a social phenomenon and was recognized by the legislator as a legal category (...)."[35]

The current legal regime governing the homework contract is laid down in Article 303 §1 KP, which states: "The Council of Ministers shall specify, by way of regulation, the scope of the application of labor law provisions to persons performing homework, with modifications resulting from the specific conditions of this form of work." Based on this statutory delegation, the Council of Ministers issued the Regulation on the employment rights of persons performing homework.[36] This regulation specifically addresses,

30 Regulation of the Minister of Industry and Trade of 27 November 1937, issued in consultation with the Minister of Social Welfare, on defining the essential characteristics of folk industry, domestic industry, and cottage work as gainful employment excluded from industrial law regulations, Journal of Laws 1937, No. 83, item 605.

31 More broadly, on the historical approach to homework regulation, cf. Teresa Wyka, "Zatrudnienie niepracownicze na podstawie umowy o pracę nakładczą," in *System prawa pracy*, ed. Krzysztof Wojciech Baran, vol. 7, *Zatrudnienie niepracownicze* (Warszawa: Wolters Kluwer Polska, 2015), 191–93.

32 Wyka, "Społeczno-ekonomiczne przesłanki rozwoju nakładztwa w Polsce," 169.

33 Regulation of the Chairman of the Committee for Small-Scale Production of 14 May 1966 on defining the essential characteristics of homework as employment excluded from the scope of industrial law, Journal of Laws 1966, no. 18, item 117.

34 Act on Labor Code of 26 June 1974 Journal of Laws 2025, item 277, as amended.

35 Wyka, "Zatrudnienie niepracownicze na podstawie umowy o pracę nakładczą," 192.

36 Regulation on the employment rights of persons performing homework of 31 December 1975, Journal of Laws 1976, No. 3, item 19, as amended.

among other issues, the right to annual leave, remuneration, and the termination of the legal relationship.

Unfortunately, at the statutory level, the regulation concerning the homework contract remains extremely concise. Article 303 §1 KP does not define the scope of labor law provisions applicable to homework. Moreover, neither the KP nor the above-mentioned regulation clarify the semantic scope of the term "homework." The literature emphasizes that this necessitates reference to doctrinal developments, case law, and the term's colloquial understanding.[37] On that basis, M. Bosak essentially equates homework with the definition contained in Article 1(a) of ILO Convention No. 177, as mentioned above.[38]

In addition to the homework regulations, the Polish legislator introduced provisions on remote work into the Labor Code (in Chapter IIc). These provisions entered into force on April 7, 2023, replacing the previous statutory provisions on telework[39] (incorporating the legal construction of telework) and the regulations on remote work introduced under the Anti-Crisis Act during the COVID-19 pandemic.[40] According to the current Article 67(18) of the Labor Code,

> work may be performed entirely or partially at a location indicated by the employee and agreed upon with the employer on each occasion, including at the employee's place of residence, in particular using means of direct remote communication (remote work).[41]

3. Legal Nature of the Homework Contract in Visegrad Group Countries (V4)

When considering the legal nature of the homework contract, and further developing the earlier discussion on its legal regime, the first issue to be resolved is whether the homework contract constitutes a basis for establishing an employment relationship.

Employment relationship characteristics in Czech labor law are described through the concept of dependent work (Czech: *Závislá práce*). Dependent work is work that is performed in the relationship of the superior of the employer and the subordination of the employee, on behalf of the employer, according to the instructions of the employer, for the employer, and the employee performs. Such work must be performed for a wage, salary or remuneration for work at the expense and responsibility of the employer, during

---

37 Maria Bosak, "Komentarz do § 1 rozporządzenia z dnia 31 grudnia 1975 r. w sprawie uprawnień pracowniczych osób wykonujących pracę nakładczą," in *Akty wykonawcze prawa pracy. Komentarz*, ed. Krzysztof Wojciech Baran (Warszawa: Wolters Kluwer, 2016), 876.

38 Ibid.

39 According to the repealed Article 67(5) §1 KP, "work may be performed regularly outside the employer's establishment, using electronic communication means within the meaning of the provisions on the provision of services by electronic means (telework)."

40 Act on special solutions related to the prevention, counteraction, and eradication of COVID-19, other infectious diseases and crisis situations caused by them of 2 March 2020, Journal of Laws 2024, item 340, as amended.

41 Cf. Leszek Mitrus, "Pojęcie i rodzaje pracy zdalnej w świetle nowelizacji kodeksu pracy z dnia 1 grudnia 2022 r.," *Praca i Zabezpieczenie Społeczne*, no. 11 (2023): 40–48, https://doi.org/10.33226/0032-6186.2023.11.5; Ludwik Florek, "Prawne ramy pracy zdalnej," *Z Problematyki Prawa Pracy i Polityki Socjalnej* 19, no. 2 (2021): 1–14, https://doi.org/10.31261/zpppips.2021.19.06.

working hours at the workplace of the employer, or at another agreed place (§ 2 (1) and (2) CZP). The current Czech labor code regulates homework and the various ways in which work can be carried out outside the employer's premises, with one general provision. Nonetheless, the basis of performing homework is an employment contract, which regulates the conditions of performing that specific type of work. Employment relation characteristics in Slovakian labor law are described through the concept of dependent work (Slovak: *Závislá práca*). Dependent work is "work performed in a relationship of superiority of the employer and subordination of the employee, personally by the employee for the employer, under the direction of the employer, on behalf of the employer" (§ 1 (2) SZP). In Slovak regulations, both homework and telework form the basis of the employment relationship, and the parties to the employment relationship shall conclude an agreement on homework or telework in the employment contract.

Characteristics of employment relationship in Hungarian labor law are the obligation of the employee's work as instructed by the employer and the obligation of the employer to provide work for the employee and to pay wages (Section 42(2)(a) and (b) Mt). In the Hungarian labor code, homework is regulated as an atypical employment relationship that should be concluded by an employment contract, which specifies the activity to be performed by the employee, the place of work, the method and amount of reimbursement. Previously, the Hungarian doctrine considered two different approaches to homeworking. It has been pointed out that homework has many characteristics of a project contract, and that it should be considered a result-based contract. On the other hand, the high economic dependence on a single employer brings the homework employment relationship closer to the classic employment relationship. Thus, a majority approach views the homework as a "mixed" legal relationship that has characteristics of both a project contract and an employment contract.[42] T. Gyulavári argues that the homework, prior to its incorporation into the Labor Code, is a *sui generis* employment relationship, combining features of both civil contracts and employment contracts.[43] Nonetheless, the legislator has decided to include homework employment relationships under the Labor Code in the chapter on atypical employment relationships, in a partially amended version of the 1994 Decree (in the context of personal performance of work and lack of direct subordination to the employer).

Polish employment relationship is characterized as a relationship in which

> an employee assumes the obligation to perform specific work for the employer and under the employer's direction at a place and time specified by the employer, and the employer assumes an obligation to employ the employee against payment of remuneration.

[42] Cf. Katalin Dudás, "Önfoglalkoztató – kényszervállalkozó – munkavállaló. Menekülés a munkajog hatálya alól," in *Tanulmányok a munkajog jövőjéről*, eds. Réka Rácz and István Horváth (Budapest: Foglalkoztatáspolitikai és Munkaügyi Minisztérium, 2004), 168; György Kenderes, *A munkaszerződés hazai szabályozásának alapkérdései* (Miskolc: Novotni Kiadó, 2007), 155. In the doctrine the minority view attached the status of the homeworker as a specific form of employment relationship; György Kiss, *Munkajog* (Budapest: Osiris Kiadó, 2005), 120–21.

[43] Tamás Gyulavári, "A foglalkoztatási jogviszonyok új dimenziója," *Esély*, no. 1 (2011): 6–7.

Meanwhile, in Poland, it is the legislator's clear intention that the homework contract, although governed by a regulation issued under the Labor Code, does not constitute a basis for establishing an employment relationship (a person performing homework under such a contract is not considered an employee within the meaning of the Polish Labor Code).[44] According to the Polish Supreme Court, incorporating a range of employee rights into the homework contract under the 1975 Regulation does not negate its civil law character.[45] Additionally, the Supreme Court indirectly stated that the homework contract constitutes a distinct type of contract, alongside a contract for services and a project contract (Polish: *umowa o dzieło*). According to the Court, an essential element of the homework contract is the definition of a minimum monthly work requirement, thereby guaranteeing the worker a specific level of remuneration.[46] The episodic nature of the work, therefore, precludes classifying the agreement as a genuine homework relationship.[47] In a similar vein, the Supreme Court noted in another decision that the homework contract, like a project contract, is a result-based contract, which is the key distinguishing feature from an employment contract (the latter being a best-effort contract).[48]

In contrast, Polish labor law scholarship demonstrates far greater uncertainty regarding the legal nature of the homework contract. Extremely divergent views are presented – depending on which features are emphasised, opposing conclusions are drawn.[49] It has been argued, for instance, that the homework contract should be classified as a type of contract for specific work. According to P. Prusinowski, it is clear that "this obligation exhibits features characteristic of both the contract for specific work (the duty to achieve a result) and the employment contract (continuity of service provision, and risk largely borne by the principal)."[50] At the same time, the author emphasizes that "one cannot ignore the fact that this contract also possesses autonomous features. The duty of personal performance of work is limited under it (...)."[51] Other voices claim that it is not an independent contract type at all, but merely a specific subtype of various civil law service contracts.[52] According to A. Świątkowski, in a homework contract – unlike in a project contract, where the essential element is the completion of a defined result for the client – the parties agree that the homeworker will receive a specified level of remuneration for

44 The Council of Ministers has not made use of its ability to specify, by regulation, the scope of labor law provisions to persons regularly performing work on a basis other than an employment relationship or homework contract (Article 303 § 2 of the Labour Code). This provision and the closed list of legal bases for establishing an employment relationship clearly indicate that a homework contract is not among them.

45 Judgment of the Supreme Court of 9 January 2008, Ref. No. III UK 76/07, LEX no. 465905. It should be noted that in Poland, alongside employment based on an employment relationship, several forms of "non-employment work" (i.e., outside the employment relationship and the labor law regime) are permitted, including "non-employment civil law contracts."

46 Ibid. See also: judgment of the Supreme Court of 8 October 2013, Ref. No. III UK 126/12, OSNP 2014, no. 9, item 135.

47 Judgment of the Supreme Court of 22 October 2013, Ref. No. III UK 156/12, LEX no. 1463910.

48 Judgment of the Supreme Court of 8 October 2013, Ref. No. III UK 126/12, OSNP 2014, no. 9, item 135.

49 Piotr Prusinowski, "Komentarz do art. 303," in *Kodeks Pracy. Komentarz*, vol. 2, *Art. 94–304(5)*, ed. Krzysztof Wojciech Baran, 6th ed. (Warszawa: Wolters Kluwer Polska, 2022), 2275–81.

50 Ibid.

51 Ibid.

52 Judgment of the Supreme Court of 9 January 2008, Ref. No. III UK 73/07, LEX nr 356045.

the work performed; therefore, such a contract should be classified as a contract for the provision of services (as a best-effort contract and not a contract of result).[53]

The authors of this study are persuaded by a view that differs from that of the Supreme Court and parts of Polish labor law doctrine – namely, that the homework contract, due to its specifically shaped legal regime and structural resemblance to an employment relationship (in terms of how the work is performed), should be described as a labor law contract, even though it involves only a weakened form of subordination resembling, but not amounting to, that of an employment relationship – even assuming it is a result-based contract (which is by no means obvious).[54]

That said, it remains the case that while in the Czech Republic, Slovakia and Hungary homework is, in various ways, incorporated into the employment relationship (either as a specific form of work organization or as an atypical form of employment), in Poland, regardless of the specific legal framework and debates about the legal nature of the homework contract, homework remains outside the employment relationship.

When considering a homework contract as the basis for establishing an employment relationship, it is crucial to take into account the defining features of an employment relationship, such as the employee's personal work performance, their subordination to the employer's instructions, the workplace and working hours, and the nature of the work (whether it is result-based or best-effort).

To Czech's remote work, as currently that legal concept is ascending after the homework and telework, applies the standard criteria of dependent work that require the employee to perform their work personally. Slovakian regulations on homework and telework consider only dependent work performed personally within the employment relationship. Outside the scope are agreements on work performance outside the employment relationship.[55] Currently, in Hungarian labor law, the homework employment relationship is limited to a specific type of homework that requires personal performance of work.[56] The Polish Regulation on the homework contract, despite the majority consent that, in the homework relationship (as in other civil law agreements), it is permitted to seek the help of third parties, does not expressly state whether the work should be carried out personally. However, in the authors' view, the Regulation includes provisions that could be used to argue that homework is personally performed work. For instance, a homework contract can be terminated without notice if there is a serious breach of obligations, faulty work performance, non-compliance with health and safety rules or if the agreed work has not been carried out for three months (§ 6 (1)). The personal nature

53 Andrzej Marian Świątkowski, "Komentarz do art. 303," in *Kodeks Pracy. Komentarz*, 5th ed., eds. Andrzej Marian Świątkowski (Warszawa: C.H. Beck, 2016), 1567; affirmatively see: Artur Rycak, "Komentarz do art. 303," in *Kodeks Pracy. Komentarz*, 34th ed. (Warszawa: C.H. Beck, 2025), Legalis; contrary view – cf., Judgment of the Supreme Court of 1 July 2020, Ref. No. I UK 400/18, LEX no. 3054431.

54 Mieczysław Piekarski and Adam Żabski, *Umowa o pracę nakładczą* (Warszawa: Instytut Wydawniczy Związków Zawodowych, 1986), 51–61; Prusinowski, "Komentarz do art. 303"; Michał Barański, "Nienazwane umowy o świadczenie pracy na gruncie prawa pracy," *Rejent*, no. 11 (2012): 9–29; Michał Barański, "Praca zdalna a umowy cywilnoprawne," in *Praca zdalna w polskim systemie prawa pracy*, ed. Małgorzata Mędrala (Warszawa: Wolters Kluwer, 2021).

55 Barancová, "Nová právna úprava domáckej práce a telepráce," 5–6.

56 Gyulavári, "A foglalkoztatási jogviszonyok új dimenziója," 4.

of the contract is further supported by homeworkers' entitlement to annual paid holiday leave (§ 14) and to maternity leave for pregnant women (§ 18). Furthermore, an employer's right to terminate a contract with a homeworker who is a trade union board member is restricted and requires union consent, unless specific conditions apply (§ 5(3)). In terms of occupational health and safety, employers must reassign homeworkers who, based on a medical certificate, develop symptoms of an occupational disease to work free from the harmful factor (§ 24 (2)). Furthermore, if a homeworker is unable to perform their previous duties due to an accident at work or an occupational disease, the employer must provide them with other suitable work (§ 25). Conversely, homeworkers can terminate their contract without notice if their health is negatively affected by their work and the employer fails to provide suitable alternative work within a month (§ 8(1)).

Regarding subordination in Czech labor law, an employee performing remote work is in a relationship of superior-subordinate between the employer and the employee; work performed during working hours at the employer's workplace or at another agreed location. However, due to the nature of remote work, the place of work can be only another agreed location, which may differ from the employee's typical homework premises, which were the employee's home. Regarding the working time, Article 87a allows the employee to define their own working time. The two classical indicators of subordination (workplace and work time) in remote work are strictly limited, or absent altogether.

According to Slovak labor law, an employee who performs homework or telework is merely subordinated to the employer, primarily because the work is performed regularly outside the employer's premises. An employee could agree in the employment contract that his work is performed in whole or in part at a place designated by the employee, if the nature of the work permits. Additionally, because the employer's right to control is restricted by the performance of work outside his workplace, an employer and employee may also agree that the employee will independently schedule his work time or that the work will be performed flexibly. As H. Barancová points out,

> when homeworking or teleworking in the form of self-scheduling by the employee, the employee is responsible for the result of the work and not for the way in which the working time is organized that leads to the result of the work.[57]

This is further strengthened by the amendment to the Slovak Labor Code, which came into force on January 1, 2026[58] and changed the criteria for defining dependent work. Therefore, the criterion of performing work at a time determined by the employer has been removed.[59]

Regarding employee subordination, Section 198(1) Mt., in its textual meaning, allows homework employment for work that can be performed independently by the employee. In most situations, if not agreed differently, the employee uses his one means

[57] Barancová, "Nová právna úprava domáckej práce a telepráce," 12.

[58] 261/2025 Z. Z Act of 24 September 2025, amending certain acts in connection with the consolidation of public finances.

[59] Cf. Ivana Glazelová, "Tretí balík konsolidačných opatrení – prehľad zmien," *Dane a Účtovníctvo v Praxi* 12 (2025).

of production, and the necessary materials are provided by the employer. Moreover, the workplace is the employee's place of residence or another place determined by the parties. The employer has a limited right to control the employee's work performance, extending only to determining the techniques and methods of work. Thus, the scope of an employee's organizational subordination in a homework relationship is limited and attenuated compared to a classic employment relationship; nonetheless, it is not an obstacle to including the homework relationship within labor and employment law.[60]

The Polish Regulation on the homework contract presents a limited personal subordination of the homeworker, but organizationally, the homeworker can be seen as economically dependent and subordinated to the employer. That is reflected in the fact that the employer is obliged to provide the homeworker with materials, as well as tools, machines and equipment necessary to perform the homework (§ 11 (1)). The employer is obliged to show concern for safe and hygienic working conditions, which involves, in particular, issuing instructions to remedy any identified deficiencies in this regard and monitoring their implementation (§ 21 (2)). In an employer's organization, if there are at least 20 homeworkers, work regulations for contract work must be established. Work regulation should specify the mutual obligations of the employer and the homeworker, in particular the rules and procedure for the allocation of work, payment and reimbursement methods, material and end-product logistics, etc. (§ 31 (2)).

When we discuss remuneration under Czech labor law, remote work, as dependent work, must be performed for a wage, salary, or remuneration under an agreement. Wages and salaries shall be paid according to the complexity, responsibility, and exertion of the work, as well as the difficulty of the working conditions. Additionally, it should be noted that the work performance and results achieved (§109(4) CZP). The remuneration from an agreement is a monetary payment provided for work performed based on an agreement to perform work or an agreement on work activity (§ 109(5) CZP).

In the Slovak regulation for homeworkers and teleworkers, as for the regular employee according to § 119(3) SZP, the employer shall agree in particular on the forms of remuneration for employees; the amount of the basic component of the salary and other components of benefits provided for work and the conditions of their provision. The basic component of the wage is the component provided according to time worked or performance achieved.

Homework in Hungarian labor law retained its characteristic features regarding the way of performance. Renumeration is calculated exclusively on performance-based wages. However, for employees whose wages are performance-based, a guaranteed wage of at least half the base wage is to be established. Moreover, if an employee's work does not meet the required quality standards due to their own fault, they typically do not receive remuneration or expense reimbursement. However, if the employer can still make use

[60] See also: Nóra Jakab, "Munkavégzők a munkavégzési viszonyok rendszerében," *Jogtudományi Közlöny*, no. 9 (2015): 427–28.

of the work, even if it is imperfect, the employee keeps the right to compensation, which is reduced proportionately.[61]

In favor to consider the homework contract in Polish context as a best-effort contract is fact that Regulation on homework contract mandates the homeworker will receive a specified level of remuneration for the work output of at least 50% of the minimum wage, however if it's their primary and sole income source it should be set no less than the minimum wage (§ 3 (1)). Moreover, a homeworker is entitled to remuneration for the work performed; nonetheless, when justified by the type of work, it's possible to use another appropriate form of remuneration for this work, as specified in the contract or in the rules for remunerating homeworkers applicable at the given employer (§ 12).[62] The employer may terminate the contract without notice due to the homeworker's fault in the event of a serious breach of his obligations under the contract, in particular, faulty carry out of the work assigned to him through his own fault (§ 6 (1)(1)). Furthermore, the liability regime for homeworkers in the event of damage resulting from the improper or non-performance of contractual obligations, or from damage to entrusted property, is designed in the same way as that for employees towards their employer (§ 30).

In the context of the legal nature of homework in V4 countries, it is worth noting the amendments to telework legislation in Hungary and Poland. Firstly, we discuss the Hungarian amendment passed in 2021. The changes to the definition of telework were dictated by a state of emergency declared as a consequence of COVID-19. The previous definition of telework highlighted the regularity of work performed away from the employer's premises, using computer equipment and with the obligation to send the results of this work electronically. Under Government Decree on the application of rules related to teleworking during the state of emergency[63] and the subsequent confirmation of the telework paradigm shift through the amendment of Mt., telework began to come closer in subject matter to homework. Under the current regulation, teleworking means that the employee works from a location other than the employer's premises for some or all of their working time. Both the criterion of regularity of teleworking[64] and the use of electronic devices and data transmission for teleworking were removed from the definition of teleworking. Thus, this leads us to the observation that, as the regulation currently

61 Anna Kozma, György Lőrincz, and Paul Lajos, *A Munka Törvénykönyvének magyarázata*., Második, aktualizált kiadás, ed. Zoltán Petrovics (Budapest: Orac Kiadó, 2023).

62 It is worth mentioning that §12 also regulates rules regarding the protection of homeworkers' remuneration, specifically referring to remuneration for work performed personally (or, in the event of illness, remuneration during periods of incapacity for work), as if they were employees.

63 Government Decree 487/2020 (XI. 11.) on the application of rules relating to remote working during emergencies.

64 Although it is noted that regularity – and consequently, the continuity of work – is embedded in the organizational subordination characteristic of telework (cf. Zoltán Bankó, "A távmunka és az úgynevezett 'home office' munkavégzés szabályozásának helyzete Magyarországon," in *Visegrád 17.0. A XVII. Magyar Munkajogi Konferencia Szerkesztett Előadásai*, eds. Lajos Pál and Zoltán Petrovics [Budapest: Wolters Kluwer, 2020], 76; an opposing view is presented, for instance, by T. Gábor Fodor and Kristóf Tóth, "Occam borotvája, avagy a 'home office' mint a munkajog unikornisa," *Munkajog*, no. 4 [2021]: 36).

stands, the differences originally defining both telework and homework are beginning to converge, if not to blur completely.[65]

At the same time, the recent introduction into the Polish Labor Code of the entirely new legal construction of remote work (replacing telework), as discussed earlier in this study, has further intensified the fundamental uncertainties regarding homework in Poland. While telework, as a flexible form of work organization, was defined as work regularly performed outside the employer's establishment using only electronic communication tools, remote work not only absorbed the legal structure of telework but also extends to include the performance of material production or service tasks. It should be noted, however, that even during the period in which telework was regulated, it was emphasised that it shared "certain essential similarities with homework arrangements, in which work is regularly performed outside the workplace."[66] In the legal literature, it is noted that the introduction of remote work into the Polish legal system has, in specific factual circumstances, led to significant difficulties in distinguishing remote work from homework.[67] For both legal constructs, the key issue is whether the physical tasks in question can, in fact, be performed – above all – in a home-based environment. Yet in individual cases, it is often difficult to verify that remote work is genuinely performed under subordination and personally, and thus within the employment relationship.[68] One might even speculate that, in introducing the provisions on remote work (as a specific form of work organization within the employment relationship), the Polish legislator may have overlooked the need to repeal or amend the existing homework regulation. Ultimately, aside from the practical challenges, when comparing remote work (performed within the employment relationship) with homework (which exists outside of it), it becomes clear that it is up to the parties themselves to choose the basis of employment – guided more by the manner in which the work is performed than by its subject matter.[69]

4. Conclusion

To summarize the above, the Czech Republic, Slovak Republic and Hungary have not only incorporated homework into the labor law framework initially through Regulations and later in the Labor Codes, but also included homeworking into the employment relationship, qualifying it as a separate way of organizing subordinate work performed outside the workplace. In Poland, despite uncertainties about the very nature of the legal relationship (civil law contract or labor law contract that are not the basis of the employment relationship), homework has developed strong links with labor law through the regulation

65 Zoltán Bankó, "Section 198."

66 Walerian Sanetra, "Komentarz do art. 303," in Józef Iwulski and Walerian Sanetra, *Kodeks pracy. Komentarz*, 3rd ed. (Warsaw: LexisNexis, 2013), LEX/el.

67 Barański, "Praca zdalna a umowy cywilnoprawne," 234; see also: Michał Barański, "Praca zdalna w czasach COVID-19," in *Moda i design w świecie COVID-19*, vol. 7, eds. Marlena Jankowska and Mirosław Pawełczyk (Katowice: Instytut Prawa Gospodarczego Sp. z o.o., 2020), 467.

68 Ibid.

69 Judgment of the Supreme Court of 13 April 2000, I PKN 594/99, OSNP 2001, no. 21, item 637; see also: Barański, "Praca zdalna a umowy cywilnoprawne," 236.

of Article 303 KP, which delegates to the Council of Ministers the obligation to determine the conditions for performing homework.[70]

Homeworking in the Czech Republic, Slovakia, and Hungary is regulated in a way that identifies the typical characteristics of the employment relationship, while preserving the distinctive features of this type of work. The most profound integration of contract work into the employment relationship can be observed in the Czech Republic, where remote work is regulated under § 317 CZP (Chech: *práce na dálku*). At the time of the adoption of the new Labour Code in 2006, newly regulated telework (albeit without the characteristics contained in the framework agreement on telework) absorbed homeworking and modernized work performed outside the employer's premises.

Both Slovakia and Hungary have retained the concept of teleworking in their labor codes, but with some distinctions. Slovakia has adopted a solution that regulates homeworking and teleworking in a single provision, which differentiates between two distinct forms of work performance (with or without electronic devices and an obligation to regularly send work results), but, in practice, grants both home workers and teleworkers the same rights and obligations. Hungary, at the same time, separates telework from homework in a chapter that regulates "atypical employment relationships." However, telework currently, without classical obligations of telework (using an electronic device and the obligation to regularly send results of work) raises the question about the sense of separation of the two institutions. The legislator should consider regulating remote work to cover both telework and homework, especially with protective measures for former homeworkers.

Poland, as an exception in V4, has not included homework in the employment relationship. At the same time, it regulated telework in accordance with the framework agreement on telework and, recently, introduced the regulation of remote work into the Polish legal order, which constructively absorbed telework. Even though the parties concerned are the ones who choose the basis of employment, guided in this respect by the directive of the manner in which the activities are performed rather than their object, at a practical level, due to the limited possibilities of verifying the actual manner in which the work is performed, such regulatory dualism represents a legislative flaw in the legislative act.

The cited regulations indicate that contractual work in the Czech Republic and Slovakia is of a best-efforts character. However, for clarity, the Hungarian regulation of homework provides a particular exception. For instance, provisions regarding remuneration, which is a performance-based wage expressly included in the employment contract and that shifts the burden of liability when we talk about the results of the work.[71] Nonetheless, as we previously mentioned, the peculiarities of the homework relationship were incorporated by the lawmakers into the employment relationship and the Hungarian labor code, as the subordination of the worker and economic dependence predominated over

[70] This is particularly evident when considering the standards of the aforementioned ILO Home Work Convention.

[71] However, when we consider Polish regulation regarding the employee's liability for damage (Article 82 KP), it shows many similarities with the Hungarian regulation regarding homework.

the classically understood employment relationship. In Poland, the legal nature of the homework contract in this respect remains highly ambiguous. The prevailing view is that the homework contract constitutes a result-based contract (as opposed to the employment contract, which is considered a best-effort contract). Contrary to the position of the Polish Supreme Court and some representatives of labor law doctrine, the authors of this study believe that arguments can be made in favor of classifying the homework contract as a best-effort contract (in line with A. Świątkowski). The presented analysis of the regulation on homework contracts confirmed not only that the homework contract has features of a best-effort contract, but also that the work shall be performed personally. The authors take the view that, in the case of homework regulation, the regime of that relationship and its protective provisions shaped the nature of the homework relationship differently from how it is commonly presented in academia. Homeworker's personal and economic dependence, with explicitly regulated personal protective provisions regarding the leaves, occupational health and safety or liability for contractual damage, explains the specific placement of homework regulations within the Polish Labor Code. That structural similarities with the employment contract only strengthen the argument that the homework contract should be regarded as a labor law contract – albeit one that does not establish an employment relationship.

The authors' research into homeworking regulations and their historical evolution in V4 countries suggests that homeworking is a step towards more flexibly reshaping traditional employment relationships, particularly regarding the place of work and work organization processes. This is evident in the Czech Republic and Slovakia, and, following the amendment to the definition of teleworking, in Hungary as well. The current Polish regulations – marked by an inexplicable dualism consisting of the coexistence, within the labor law system, of provisions on remote work (within the employment relationship) and homework (outside the employment relationship) – give rise to virtually irresolvable practical problems and require immediate legislative intervention. Following L. Mitrus, it should be noted that a new perspective on the concept of the employment relationship is needed, and it would be desirable to amend, among other things, the Polish definition of the employment relationship to reflect the nature of long-distance work.[72] Assuming the definition of the employment relationship in Poland is expanded, while still maintaining the absolute requirement of personal performance of work within that legal relationship, the provisions concerning homework should be largely replaced by the statutory regulation of remote work. Only work corresponding to the current model of homework, performed with the help of other persons, could continue to fall outside the scope of employment – possibly with the appropriate application of selected labor law provisions.[73] In Poland,

> remote work constitutes yet another example of the normative convergence of employment and non-employment constructions that enable the performance of work outside the employment

[72] Leszek Mitrus, "Praca zdalna *de lege lata* i *de lege ferenda* – zmiana miejsca wykonywania pracy czy nowa koncepcja stosunku pracy? Część 2," *Praca i Zabezpieczenie Społeczne* 11 (2020): 3–10, https://doi.org/10.33226/0032-6186.2020.11.1.

[73] Barański, "Praca zdalna a umowy cywilnoprawne," 237–38.

> relationship. Considering that civil-law employment in its current scope is undesirable, the statutory regulation of remote work could significantly reduce its prevalence.[74]

The reduction of disparities in the attractiveness of civil-law employment should be achieved, among other things, by increasing labor law's flexibility.[75]

> [Since] the relationships between the parties to the employment relationship are evolving towards organizational subordination, in which the strictly hierarchical model of work performance is losing significance, the shape of labor law must be adjusted to the current needs of the labor market.[76]

The analysis, particularly from the perspective of Polish labor law, demonstrates the continued relevance of homework and its relationship with remote/teleworking. Despite the previously mentioned minor significance of homework, maintaining a legal dualism for homework and remote work does not promote regulatory certainty. Examples from V4 countries clearly highlight issues with Polish regulations and could encourage a responsible approach to addressing this matter. To achieve the aims of labor law, which are to regulate subordinated employment relationships and ensure human rights in employment, the legislator should take legal action to address the current situation.

References

Bankó, Zoltán. "A távmunka és az úgynevezett 'home office' munkavégzés szabályozásának helyzete Magyarországon." In *Visegrád 17.0. A XVII. Magyar Munkajogi Konferencia Szerkesztett Előadásai*, edited by Lajos Pál and Zoltán Petrovics, 65–89. Budapest: Wolters Kluwer, 2020.

Barancová, Helena. "Nová právna úprava domáckej práce a telepráce." *Právny Obzor* 105, no. 1 (2022): 3–18. https://doi.org/10.31577/pravnyobzor.2022.1.01.

Barański, Michał. "Employment Flexibility in Times of Crisis." *Studia Iuridica*, no. 95 (2023): 9–29. https://doi.org/10.31338/2544-3135.si.2022-95.1.

Barański, Michał. "Nienazwane umowy o świadczenie pracy na gruncie prawa pracy." *Rejent*, no. 11 (2012): 9–29.

Barański, Michał. "Praca zdalna a umowy cywilnoprawne." In *Praca zdalna w polskim systemie prawa pracy*, edited by Małgorzata Mędrala, 231–39. Warszawa: Wolters Kluwer, 2021.

Barański, Michał. "Praca zdalna w czasach COVID-19." In *Moda i design w świecie COVID-19: koronakryzys przyczynkiem do refleksji prawniczej, technologicznej i socjologicznej*, vol. 7, edited by Marlena Jankowska and Mirosław Pawełczyk, 272–81. Katowice: Instytut Prawa Gospodarczego Sp. z o.o., 2020.

Bosak, Maria. "Komentarz do § 1 rozporządzenia z dnia 31 grudnia 1975 r. w sprawie uprawnie pracowniczych osób wykonujących pracę nakładczą." In *Akty wykonawcze prawa pracy. Komentarz*, edited by Krzysztof Wojciech Baran, 875–924. Warszawa: Wolters Kluwer, 2016.

Dandová, Eva. "Práce na dálku." *BHP. – Bezpečnost a Hygiena Práce*, no. 7/8 (2025): 14–17.

[74] Barański, "Praca zdalna a umowy cywilnoprawne," 238.

[75] Izabela Florczak, "Granice rozszerzania instytucji prawa pracy na zatrudnienie cywilnoprawne," *Folia Iuridica Universitatis Wratislaviensis* 4, no. 1 (2015): 249.

[76] Barański, "Praca zdalna a umowy cywilnoprawne," 238.

Dudás, Katalin. "Önfoglalkoztató – kényszervállalkozó – munkavállaló. Menekülés a munkajog hatálya alól." In *Tanulmányok a munkajog jövőjéről*, edited by Réka Rácz and István Horváth, 143–76. Budapest: Foglalkoztatáspolitikai és Munkaügyi Minisztérium, 2004.

Florczak, Izabela. "Granice rozszerzania instytucji prawa pracy na zatrudnienie cywilnoprawne." *Folia Iuridica Universitatis Wratislaviensis* 4, no. 1 (2015): 237–52.

Florek, Ludwik. "Prawne ramy pracy zdalnej." *Z Problematyki Prawa Pracy i Polityki Socjalnej* 19, no. 2 (2021): 1–14. https://doi.org/10.31261/zpppips.2021.19.06.

Fodor, T. Gábor, and Kristóf Tóth. "Occam borotvája, avagy a 'home office' mint a munkajog unikornisa." *Munkajog*, no. 4 (2021): 34–38.

Giedrewicz-Niewińska, Aneta, Viktor Križan, and Jana Komendová. "The Obligations of the Employer in the Implementation of Remote Work: The Examples of Slovakia, the Czech Republic and Poland." *Białostockie Studia Prawnicze* 29, no. 2 (2024): 83–97. https://doi.org/10.15290/bsp.2024.29.02.07.

Glazelová, Ivana. "Tretí balík konsolidačných opatrení – prehľad zmien." *Dane a Účtovníctvo v Praxi* 11 (2025).

Gyulavári, Tamás. "A foglalkoztatási jogviszonyok új dimenziója." *Esély*, no. 1 (2011): 3–23.

Homer, Zuzana. "Výkon domácej práce a telepráce v kontexte aktuálnej aplikačnej praxe." In *Zamestnanec v digitálnom prostredí*, edited by Monika Minčičová, Marcel Dolobáč, and Jana Žuľová, 112–22. Košice: Univerzita Pavla Jozefa Šafárika, 2021.

Jakab, Nóra. "Munkavégzők a munkavégzési viszonyok rendszerében." *Jogtudományi Közlöny*, no. 9 (2015): 421–32.

Kenderes, György. *A munkaszerződés hazai szabályozásának alapkérdései*. Miskolc: Novotni Kiadó, 2007.

Kiss, György. *Munkajog*. Budapest: Osiris Kiadó, 2005.

Kozma, Anna, György Lőrincz, and Paul Lajos. *A Munka Törvénykönyvének magyarázata*, edited by Zoltán Petrovics. Budapest: Orac Kiadó, 2023.

Matlovičová, Iveta. "Pravidelná a príležitostná práca z domácnosti zamestnanca." *Dane a Účtovníctvo v Praxi* 26, no. 5 (2021): 47–53.

Mitrus, Leszek. "Pojęcie i rodzaje pracy zdalnej w świetle nowelizacji kodeksu pracy z dnia 1 grudnia 2022 r." *Praca i Zabezpieczenie Społeczne*, no. 11 (2023): 40–48. https://doi.org/10.33226/0032-6186.2023.11.5.

Mitrus, Leszek. "Praca zdalna *de lege lata* i *de lege ferenda* – zmiana miejsca wykonywania pracy czy nowa koncepcja stosunku pracy? Część 2." *Praca i Zabezpieczenie Społeczne* 11 (2020): 3–10. https://doi.org/10.33226/0032-6186.2020.11.1.

Pichrt, Jan. "Několik Poznámek k Pracovním Vztahům Domovníků, Obchodních Pomocníků a Domáckýchzaměstnanců v Období První Republiky." In *Caro Amico: 60 Kapitol pro Michala Skřejpka Aneb Římské Právo Napříč Staletími*, edited by Petr Bělovský and Kamila Stloukalová, 312–23. Praha: Auditorium, 2017.

Piekarski, Mieczysław, and Adam Żabski. *Umowa o pracę nakładczą*. Warszawa: Instytut Wydawniczy Związków Zawodowych, 1986.

Prusinowski, Piotr. "Komentarz do art. 303." In *Kodeks Pracy. Komentarz*. Vol. 2, *Art. 94–304(5)*, 6th ed., edited by Krzysztof Wojciech Baran, 2275–81. Warszawa: Wolters Kluwer Polska, 2022.

Rycak, Artur. "Komentarz do art. 303." In *Kodeks Pracy. Komentarz*, 34th ed., edited by Krzysztof Walczak, 1–7. Warszawa: C.H. Beck, 2025. Legalis.

Sanetra, Walerian. "Komentarz do art. 303." In *Kodeks pracy. Komentarz*, 3rd ed., edited by Józef Iwulski and Walerian Sanetra, 1–5. Warsaw: LexisNexis, 2013. LEX/el.

Štefko, Martin. "§ 317." In *Zákoník Práce. Komentář*, edited by Miroslav Bělina and Ljubomír Drápal, 1254–58. Praha: C.H. Beck, 2019.

Toman, Jozef. "§ 52. Domácka práca a telepráca." In *Zákonník práce, Zákon o kolektívnom vyjednávaní – Komentár*, 5th ed., edited by Marek Švec and Jozef Toman, 509–36. Bratislava: Wolters Kluwer 2023.

Świątkowski, Andrzej Marian. "Komentarz do art. 303." In *Kodeks Pracy. Komentarz*, 5th ed., edited by Andrzej Marian Świątkowski, 1565–78. Warszawa: C.H. Beck, 2016.

Vallas, Steven, and Juliet B. Schor. "What Do Platforms Do? Understanding the Gig Economy." *Annual Review of Sociology* 46, no. 1 (2020): 273–94. https://doi.org/10.1146/annurev-soc-121919-054857.

Vysokajová, Margerita. "§ 317." In *Zákoník práce: komentář*, edited by Petr Hůrka, Nataša Randlová, Jiří Doležílek et al., 731–36. Praha: Wolters Kluwer, 2025.

Wyka, Teresa. "Społeczno-ekonomiczne przesłanki rozwoju nakładztwa w Polsce." *Z Problematyki Prawa Pracy i Polityki Socjalnej*, no. 3 (1980): 168–89.

Wyka, Teresa. "Sytuacja prawna osób wykonujących pracę nakładczą." *Acta Universitatis Lodziensis. Folia Iuridica* 25 (1986): 3–128.

Wyka, Teresa. "Zatrudnienie niepracownicze na podstawie umowy o pracę nakładczą." In *System prawa pracy*. Vol. 7, *Zatrudnienie Niepracownicze*, edited by Krzysztof Wojciech Baran, 191–219. Warszawa: Wolters Kluwer Polska, 2015.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 87–101
https://doi.org/10.31743/recl.19141
Received: 17 October 2025 | Accepted: 25 February 2026 | Published: 31 March 2026

The Baby Hatch at the Crossroads of Human Rights

Stjepan Novak
PhD, Ministry of the Internal Affairs, Republic of Croatia; correspondence address: Ulica grada Vukovara 33, Zagreb, Republic of Croatia; e-mail: stjepannovak@hotmail.com
https://orcid.org/0000-0002-6600-4974

Antonija Novak
Mag. paed. relig. et catech, Elementary school Ivanja Reka, Ivanja Reka-Zagreb, Republic of Croatia; correspondence address: Ivanjorečka cesta 1b, Zagreb, Republic of Croatia; e-mail: antonija.novak2@skole.hr

Abstract: When the baby hatch (known as "Window of Life") came under public scrutiny in the Republic of Croatia, it was met with a number of criticisms. The most prominent among them were its lack of regulation under Croatian law, the alleged encouragement of committing a criminal offense, and the violation of the child's right to identity. Neither the concept of the baby hatch, nor the criticisms directed at this method of caring for unwanted newborns are new in Europe or beyond, nor are they unfamiliar to the case law of the European Court of Human Rights. This paper will attempt to demonstrate that the only well-founded objection is the lack of adequate legal regulation. The claim that the existence of the baby hatch encourages criminal behavior is simply unfounded, while the potential violation of the child's right to know their identity can be justified by the protection of a higher right – the right to life.

Keywords: baby hatch, right to life, right to private life, anonymous childbirth, rights of the child

1. Introduction

The baby hatch can most simply be defined as a place where unwanted newborns are left. Variants of this concept have existed since the medieval period, and today, they can be found around the world. In a broader sense, it is one of the methods of caring for unwanted children, whose mothers typically do not wish to keep the child but do wish to remain anonymous. This absolute and impenetrable anonymity is precisely what constitutes its *differentia specifica* when compared to the other two main forms of caring for unwanted children: the institute of anonymous childbirth, which guarantees the mother's anonymity to a certain degree, and the typical USA[1] legal framework known as safe haven laws.

Among these mechanisms, the baby hatch is the most controversial and most frequently criticized, as it provides no even minimal state oversight. The core of this issue lies in the neglect of the child's right to know its own identity, as well as in the fact that, due to the absence of any legal regulation concerning baby hatches, abandoning a child – even in such a place – constitutes a criminal offense.

This paper aims to examine the validity of these criticisms in light of the primary purpose of the baby hatch – saving lives.

[1] Kevin Browne, Shihning Chou, and Kate Whitfield, *Child Abandonment and Its Prevention in Europe* (Nottingham: The University of Nottingham, 2012), 17.

ISSN 2545-384X (Online)

2. Models of Care for Unwanted Children as an Alternative to Abortion or Infanticide

Anonymous childbirth is particularly regulated in France under the term *accouchement sous X* and has even undergone review by the European Court of Human Rights (hereinafter: ECtHR) in the case *Odièvre v. France*.[2] This system balances the woman's interest in remaining anonymous with the child's interest in obtaining information about the child's origin. The woman can "cover" her personal data, and the child may access this information with her consent, provided she is informed about the consequences of her request for anonymity, as well as the child's rights to access data about the mother that does not allow identification.[3] In this process, a state council, a specialized public body, acts as an intermediary between the woman and the child. On the other hand, the anonymous childbirth system in Italy did not satisfy the ECtHR in the case of *Godelli v. Italy*,[4] since in that system an adopted child who was not recognized at birth may access non-identifying information about their origin or request the identity of their mother, only after 100 years.[5] Consequently, Italian constitutional court practice[6] and expected legislative changes should, if enacted,[7] correct the imbalance between the woman's right to anonymity and the child's right to access relevant information.[8] In systems with a regulated institute of anonymous or confidential childbirth, criminal liability for the woman who chooses this option does not arise.[9] In Italy, France, Austria, and Luxembourg, the presumption of maternity, as known in Croatian law, does not exist; a woman's consent is required for her to be registered in the relevant state registry as the child's mother.[10] The Committee on the Rights of the Child (hereinafter: the Committee) has expressed concern regarding anonymous

2 European Court of Human Rights, ECtHR Judgment of 13 February 2003, Case Odièvre v. France, application no. 42326/98, hudoc.int.

3 Nenad Hlača, "Pravo majke na anonimnost poroda – 'L'accouchement sous X – Porod pod X'," *Gynaecologia et Perinatologia* 16, no. 3 (2007): 159.

4 ECtHR Judgment of 25 September 2012, Case Godelli v. Italy, application no. 33783/99, hudoc.int.

5 European Court of Human Rights (ECtHR), *Guide to the Case-Law of the European Court of Human Rights: Data Protection* (Strasbourg: Council of Europe, 2020), para. 271.

6 Corte Costituzionale, Sentenza n. 278, 22 November 2013, accessed September 14, 2025, https://www.biodiritto.org/Biolaw-pedia/Giurisprudenza/Corte-costituzionale-sent.-n.-278-2013-accesso-dell-adottato-alle-informazioni-sull-identita-della-madre-biologica; Stefano Troiano, "Understanding and Redefining the Rationale of State Policies Allowing Anonymous Birth: A Difficult Balance Between Conflicting Interests," *International Journal of Jurisprudence of the Family* 4 (2013): 204, https://ssrn.com/abstract=322394.

7 Sabrina Praduroux, "The Right to Know One's Genetic Origins: A Right in Need of Regulation," *Italian Law Journal* 7, no. 2 (2021): 813, https://dx.doi.org/10.23815/2421-2156.ITALJ.

8 Nataša Hadžimanović, "Confidential and Anonymous Birth in National Laws: Useful and Compatible with the UN Convention on the Rights of the Child?," *Comparazione e diritto civile* (2018): 132.

9 Browne, Chou, and Whitfield, *Child Abandonment*, 31; Initiative for Reproductive Health Information (IRHI), "Anonymous Birth," accessed October 9, 2025, https://anonymegeburt.at/anonymous-birth.

10 Adéla Lemrová et al., "Anonymous Births: A Conflict of Three Rights – Which Prevails?," *Social Pathology and Prevention* 7, no. 2 (2022): 40; Tamara Mladenović, "Pravo na anonimni porođaj naspram prava deteta na identitet," *Pravni zapisi* 12, no. 2 (2021): 460, https://doi.org/10.5937/pravzap0-34192; Troiano, "Understanding and Redefining the Rationale of State Policies Allowing Anonymous Birth," 181; Valentina Colcelli, "Anonymous Birth, Birth Registration and the Child's Right to Know Their Origins in the Italian Legal System: A Short Comment," *Journal of Civil & Legal Sciences* 1 (2013): 2, https://doi.org/10.4172/2169-0170.1000101; ECtHR Judgment of 13 February 2003, Case Odièvre v. France, application no. 42326/98, para. 19, hudoc.int.

childbirth in Luxembourg, which requires the biological mother's consent as a *conditio sine qua non* for the child's access to any information related to her.[11]

Germany, as well as Slovakia,[12] recognizes so-called confidential birth, a variant of anonymous childbirth with somewhat less protection of the woman's right to anonymity. In Germany, a child can access information about their biological mother from the age of 16, after which they are obliged to leave with a professional counselor.[13] The Committee has supported the German confidential birth model,[14] and recommended it, for example, to Switzerland[15] and Hungary.[16]

"Safe haven" locations are in hospitals, police departments, or fire departments, where mothers can anonymously leave their child without fear of criminal prosecution.[17] The age at which a child can be left is not uniformly regulated across U.S. states,[18] and the mechanisms that allow the child, later in life, to access information about their origin vary from state to state as well.[19] Although quite similar to baby hatches, what distinguishes "safe haven" sites is their minimal level of institutionalization. This enables contact with professional staff, who, through appropriate consultations, can ensure the mother's safety in deciding to leave the child, provide necessary healthcare, and offer any relevant information that may assist her. Conversely, professional staff can collect data that the child might seek later in life.[20] Similar systems exist in Hungary and Slovakia, where special incubators are installed in front of hospitals, and all counseling and leaving personal data are optional.[21]

---

11 Committee on the Rights of the Child, *Concluding Observations on the Combined Third and Fourth Periodic Reports of Luxembourg, Adopted at the Sixty-Fourth Session (16 September–4 October 2013)*, UN Doc. CRC/C/LUX/CO/3–4 (Geneva: United Nations, October 29, 2013), para. 9, accessed September 14, 2025, https://digitallibrary.un.org/record/767372?v=pdf.

12 Rodovan Blažek and Margita Prokeinová, "How to Provide a Legal Safe Harbor for Mothers of Unwanted Newborns," *Issues in Law & Medicine* 32, no. 1 (2017): 64.

13 Lemrová et al., "Anonymous Births," 38.

14 Committee on the Rights of the Child, *Concluding Observations on the Combined Fifth to Sixth Periodic Reports of Germany*, UN Doc. CRC/C/DEU/CO/5–6 (Geneva: United Nations, September 23, 2022), para. 19, accessed October 9, 2025, https://unfairtobacco.org/wp-content/uploads/2022/10/CRC_Germany_Concluding-Observations_Sept2022.pdf.

15 Committee on the Rights of the Child, *Concluding Observations on the Combined Fifth and Sixth Periodic Reports of Switzerland*, UN Doc. CRC/C/CHE/CO/5–6 (Geneva: United Nations, October 22, 2021), para. 22, accessed October 9, 2025, https://digitallibrary.un.org/record/3945313?ln=zh_CN&v=pdf.

16 Committee on the Rights of the Child, *Concluding Observations on the Sixth Periodic Report of Hungary*, UN Doc. CRC/C/HUN/CO/6 (Geneva: United Nations, March 3, 2020), para. 26, accessed October 9, 2025, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2FC%2FHUN%2FCO%2F6&Lang=en.

17 Browne, Chou, and Whitfield, *Child Abandonment*, 17; Jurgita Stasiūnienė, Viktoras Justickis, and Algimantas Jasulaitis, "Newborn Murder and Its Legal Prevention," *Health Policy and Management* 1, no. 8 (2015): 112, https://doi.org/10.13165/SPV-15-1-8-05.

18 Whitney Rosenberg, "The Illegality of Baby Safes as a Hindrance to Women Who Want to Relinquish Their Parental Rights," *Athens Journal of Law* 1, no. 4 (2015): 203, https://doi.org/10.30958/ajl.1-4-1.

19 Kurium Govender, "An Ethico-Legal Case for Baby Hatches in South Africa" (MSc diss., University of the Witwatersrand, Johannesburg, 2021), 25, https://wiredspace.wits.ac.za/items/12cc9eee-b0c2-4e92-ab95-459fe5c03e50.

20 Browne, Chou, and Whitfield, *Child Abandonment*, 19; Govender, "An Ethico-Legal Case," 24.

21 Browne, Chou, and Whitfield, *Child Abandonment*, 16.

Baby hatches exist, among others, in Austria, Belgium, the Czech Republic, Italy, Latvia, Lithuania, Hungary, the Netherlands, Germany, Poland, Portugal, Russia, Slovakia, Switzerland, the United Kingdom, as well as the Philippines, India, Japan, South Korea, South Africa, and Malaysia.[22] Poland and the Czech Republic also offer accommodation services for women planning to leave their child, ensuring their anonymity upon request.[23]

As one of the most controversial methods of caring for unwanted children, they raise numerous ethical, legal, and social concerns. In the following sections, the most frequently voiced criticisms of their operation will be presented, with a systematic attempt to address each and examine its underlying rationale.

3. The Baby Hatch – The Other Side of Saving Lives

Three arguments against the baby hatch will be presented in the following chapters, and attempts will be made to respond to them.

3.1. The Right to Know One's Origins and Other Rights from the Convention on the Rights of the Child

In Germany, the right of every individual to know their origins has been established as a fundamental personal right, based on the general right to dignity and free development, by the Federal Constitutional Court in a ruling dated January 31, 1989. In Switzerland, the right of every individual to know their origins has been recognized by the Federal Constitution since 1992.[24] Nevertheless, both countries recognize the aforementioned methods of caring for unwanted newborns. There are persistent objections that baby hatches violate the Convention on the Rights of the Child from 1989 (hereinafter: the Convention).[25] In its 2011 report on the Czech Republic[26] and India,[27] the Committee on the Rights of the Child[28] expressed opposition to baby hatches, citing several provisions of the Convention. Without providing any arguments, it stated that this practice violates the provisions of Articles 6, 7, 8, 9, and 19 of the Convention. Similar views were expressed in its 2015

22 For example Blažek and Prokeinová, "How to Provide a Legal Safe Harbor," 64; Browne, Chou, and Whitfield, *Child Abandonment*, 17; Shadiya Mohamed Baqutayan et al., "Should We Maintain Baby Hatches in Our Society? Baby Hatch Policy in Malaysia," *International Journal of Academic Research in Business and Social Sciences* 12, no. 11 (2022): 3073–88, https://doi.org/10.6007/IJARBSS/v12-i11/15032.

23 Browne, Chou, and Whitfield, *Child Abandonment*, 17.

24 Dissenting opinion of Judges Wildhaber et al., ECtHR Judgment of 13 February 2003, Case Odièvre v. France, application no. 42326/98, hudoc.int.

25 United Nations Children's Fund (UNICEF), *Convention on the Rights of the Child: Full Text*, accessed October 9, 2025, https://www.unicef.org/child-rights-convention/convention-text.

26 Committee on the Rights of the Child, *Consideration of Reports Submitted by States Parties under Article 44 of the Convention: Convention on the Rights of the Child: Concluding Observations: Czech Republic*, UN Doc. CRC/C/CZE/CO/3–4 (Geneva: United Nations, August 4, 2011), para. 49, accessed October 9, 2025, https://digitallibrary.un.org/record/708485.

27 Committee on the Rights of the Child, *Concluding Observations on the Combined Third and Fourth Periodic Reports of India*, UN Doc. CRC/C/IND/CO/3–4 (Geneva: United Nations, July 7, 2014), para. 42.

28 Govender, "An Ethico-Legal Case," 17.

report concerning the Netherlands,[29] and the elimination of baby hatches was set as a goal regarding Germany,[30] Austria,[31] Czech Republic,[32] Slovakia,[33] and Hungary.[34]

In accordance with Article 6 of the Convention, states recognize the inherent right to life of every child and shall ensure, to the maximum extent possible, the survival and development of the child.

Article 7, paragraph 1, stipulates that the child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality, and, as far as possible, the right to know and be cared for by his or her parents.[35]

According to Article 8, paragraph 1, States Parties undertake to respect the right of the child to preserve his or her identity, including nationality, name, and family relations, as recognized by law, without unlawful interference.[36]

Article 9, paragraph 1, states that States Parties shall ensure that a child shall not be separated from his or her parents against their will, except when competent authorities subject to judicial review determine, in accordance with applicable law and procedures, that such separation is necessary for the best interests of the child. Such determination may be necessary in a particular case, such as one involving abuse or neglect of the child by the parents, or one where the parents are living separately and a decision must be made as to the child's place of residence.[37]

---

29 Committee on the Rights of the Child, *Concluding Observations on the Fourth Periodic Report of the Netherlands*, UN Doc. CRC/C/NLD/CO/4 (2015), para. 35, accessed October 9, 2025, https://docs.un.org/en/CRC/C/NLD/CO/4, para. 35.

30 Committee on the Rights of the Child, *Concluding Observations on the Combined Fifth to Sixth Periodic Reports of Germany*, 2022, para. 19.

31 Committee on the Rights of the Child, *Concluding Observations on the Combined Fifth and Sixth Periodic Reports of Austria*, UN Doc. CRC/C/AUT/CO/5–6 (Geneva: United Nations, March 6, 2020), para. 20.

32 Committee on the Rights of the Child, *Concluding Observations: Czech Republic*, 2011, para. 50.

33 Committee on the Rights of the Child, *Concluding Observations on Slovakia*, UN Doc. CRC/C/15/Add.140 (Geneva: United Nations, April 9, 2014), para. 18.

34 Committee on the Rights of the Child, *Concluding Observations on the Sixth Periodic Report of Hungary*, 2020, para. 26.

35 Article 7(2), Convention on the Rights of the Child: "States Parties shall ensure the implementation of these rights in accordance with their national law and their obligations under the relevant international instruments in this field, in particular where the child would otherwise be stateless."

36 Article 8(2), Convention on the Rights of the Child: "Where a child is illegally deprived of some or all of the elements of his or her identity, States Parties shall provide appropriate assistance and protection, with a view to re-establishing his or her identity speedily."

37 Article 9(2–4), Convention on the Rights of the Child: "2. In any proceedings pursuant to paragraph 1 of the present article, all interested parties shall be given an opportunity to participate in the proceedings and make their views known. 3. States Parties shall respect the right of the child who is separated from one or both parents to maintain personal relations and direct contact with both parents on a regular basis, except if it is contrary to the child's best interests. 4. Where such separation results from any action initiated by a State Party, such as the detention, imprisonment, exile, deportation or death (including death arising from any cause while the person is in the custody of the State) of one or both parents or of the child, that State Party shall, upon request, provide the parents, the child or, if appropriate, another member of the family with the essential information concerning the whereabouts of the absent member(s) of the family unless the provision of the information would be detrimental to the well-being of the child. States Parties shall further ensure that the submission of such a request shall of itself entail no adverse consequences for the person(s) concerned."

According to Article 19, paragraph 1, States Parties shall take all appropriate legislative, administrative, social, and educational measures to protect the child from all forms of physical or mental violence, injury, or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s), or any other person who has the care of the child.[38]

The Committee on the Rights of the Child failed to explain how baby hatches violate the aforementioned articles. The baby hatch in no way threatens a child's right to life, survival, and development; on the contrary, by its very purpose, it supports these rights. Moreover, the phrase stating that states "shall ensure, to the maximum extent possible, the survival and development of the child" could actually serve as a justification for the existence of baby hatches, or even as an argument in their favor.[39] The words "to the maximum extent possible" could be interpreted as "under all circumstances," "at any cost," or similar, and in any case imply an absolute priority. In contrast, the words "if possible" from Article 7 of the Convention carry a different meaning, indicating a relative nature of the provision, as opposed to the absolute nature characterizing Article 6.

Objections based on disagreement with Article 7 of the Convention can, once again, be dismissed by the logic of the primacy of the right to life.

As early as *Gaskin v. the United Kingdom*,[40] the ECtHR recognized that access to information concerning one's childhood and origins falls within the scope of "private life," emphasizing the vital interest protected by Article 8 in obtaining information necessary to understand one's personal history and identity. In *Mikulić v. Croatia*,[41] the ECtHR stressed that uncertainty as to one's personal identity, including paternity, engages Article 8 and that States must provide effective and timely procedures enabling the determination of such claims. The importance of the child's interest in knowing the truth about his or her origins was accorded decisive weight in *Mandet v. France*.[42] Based on this case-law,[43] it can be argued that the ECtHR has consistently held that respect for private life requires that everyone should be able to establish details of their identity as an individual human being, which includes knowledge of one's parentage and the legal parent–child relationship. Nevertheless, it is not absolute.

Asai and Ishimoto write that fixating exclusively on respecting the right of the child to know his or her parents without considering the circumstances will lead to violation of the right to life, which is a condition *sine qua non* for the realization of every

38 Article 19(2), Convention on the Rights of the Child: "Such protective measures should, as appropriate, include effective procedures for the establishment of social programmes to provide necessary support for the child and for those who have the care of the child, as well as for other forms of prevention and for identification, reporting, referral, investigation, treatment and follow-up of instances of child maltreatment described heretofore, and, as appropriate, for judicial involvement."

39 Rosenberg, "Illegality of Baby Safes," 207.

40 ECtHR Judgment of 7 July 1989, Case Gaskin v. the United Kingdom, application no. 10454/83, para. 37, hudoc.int.

41 ECtHR Judgment of 7 February 2002, Case Mikulić v. Croatia, application no. 53176/99, para. 66.

42 ECtHR Judgment of 14 January 2016, Case Mandet v. France, application no. 30955/12, paras 56–60.

43 European Court of Human Rights, *Guide on CaseLaw of the European Convention on Human Rights: Rights of the Child* (Strasbourg: ECtHR, 2025), accessed February 23, 2026, https://ks.echr.coe.int/documents/d/echr-ks/guide_rights_of_the_child_eng.

other right.[44] Stasiūnienė, Justickis, and Jasulaitis emphasize the same point, particularly highlighting the words from Article 7's provision: "as far as possible."[45] Hlača points out that the Convention itself relativizes the right of a child to know who their biological parents are and is not classified as one of the child's original rights.[46] Furthermore, objections regarding inconsistencies with Articles 7 and 8 fail to take into account the *travaux préparatoires* of the Convention.[47] Regarding Article 7, even at that time, the German Democratic Republic and the USSR, as well as the USA, emphasized that the "right to know one's parents" is not always feasible.[48] Other objections, or rather discussions, mostly concerned issues related to nationality.[49]

As for Article 8, it is a product of the political situation in Argentina,[50] which proposed it, and it aims to protect children separated from their parents or otherwise endangered due to war or similar circumstances.[51] From the very beginning, the article was considered redundant, even incorrect, in its definition of identity and connection through blood relations, and was accepted primarily for emotional reasons.[52]

Referring to Article 9 is especially unfounded, considering that it explicitly states that a child must not be separated from their parents against their will. In this sense, Article 9 would rather support the existence of baby hatches than oppose it. Of course, it cannot be ruled out that someone might leave another person's child in a baby hatch, for example, another family member.[53] However, the same risk should not be a reason to ban baby hatches. The same risk exists in "safe haven" systems. Abuse of any institution is a possibility, but that possibility cannot be a reason to prohibit the institution itself. After all, cases of leaving children in baby hatches are rare. So far, the only cases in the Republic of Croatia, as well as cases of leaving children in unsuitable places, have been extensively covered by the media, so reunification with the biological mother, if she wishes, is very likely.

Similarly, the reference to Article 19 of the Convention is unfounded. Provided that baby hatches are legally regulated, not only does Article 19 not oppose baby hatches in any way, but it can even be considered a measure aimed at protecting the child "from

44 Atsushi Asai and Hiroko Ishimoto, "Should We Maintain Baby Hatches in Our Society?," *BMC Medical Ethics* 14, no. 9 (2013): 2, https://doi.org/10.1186/1472-6939-14-9; Mladenović, "Pravo na anonimni porođaj naspram prava deteta," 448.

45 Stasiūnienė, Justickis, and Jasulaitis, "Newborn Murder," 113.

46 Hlača, "Pravo majke," 160.

47 Rosenberg, "Illegality of Baby Safes," 206.

48 "…the right to know one's parents could not be applied everywhere." United Nations, *Legislative History of the Convention on the Rights of the Child* (New York–Geneva: UN, 2007), 378, accessed October 9, 2025, https://digitallibrary.un.org/record/602462?v=pdf.

49 Ibid., 370.

50 Katherine O'Donovan, "'Real' Mothers for Abandoned Children," *Law & Society Review* 36, no. 2 (2002): 352; Barbara Preložnjak, "Modern Challenges in the Implementation of the Child's Right to Know His Origin," *EU and Comparative Law Issues and Challenges Series (ECLIC)* 4 (2020): 1175–203, 1178, https://doi.org/10.25234/eclic/11944; Hadžimanović, "Confidential and Anonymous Birth," 130.

51 Rosenberg, "Illegality of Baby Safes," 206.

52 O'Donovan, "'Real' Mothers for Abandoned Children," 352.

53 Troiano, "Understanding and Redefining the Rationale of State Policies Allowing Anonymous Birth," 203.

all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment, or exploitation."[54]

Furthermore, the Committee urges India "to take all necessary measures to end the practice of anonymous abandonment of children and to strengthen and promote alternatives as soon as possible" and "to increase its efforts to address the root causes of abandonment of infants, including by providing family-planning services, adequate counselling and social support for unplanned pregnancies."[55] This is, alongside the Committee's similar statements regarding the Netherlands, the Czech Republic, and Slovakia in contrast to the general position of the ECtHR in the case *Odièvre v. France*, where the avoidance of abortion was recognized as a legitimate public interest.[56]

In this regard, it is useful to emphasize the concurring opinion of Judges Ress and Kūris in *Odièvre v. France*, 2003, which states that taking appropriate measures to improve the situation of mothers in distress and to protect the lives of children by reducing the number of abortions – whether legal or illegal – as much as possible, is in the public interest.[57] A similar *ratio* can be found in the judgment of the Constitutional Court of Italy,[58] which – although the ECtHR challenged the specific judgment of that court – was not itself contested.[59]

3.2. Instigation to Commit a Criminal Offense

In the legal system of the Republic of Croatia, abandoning a child in a baby shelter or in any other place is a criminal offense. Article 176 of the Criminal Code of Republic of Croatia prescribes that "whoever deserts his or her child with the aim of permanently getting rid of him or her shall be punished by imprisonment not exceeding three years."[60] In cases where the child's parentage is not established, according to Article 181 of the Croatian Family, a child left in a baby hatch will, after a period of three months, meet the conditions for adoption.[61] If the identity of the mother is later established, she is subject to criminal prosecution. Regarding the child itself, it may be adopted if the mother and father are deprived of the right to exercise parental care,[62] since their consent for adoption is not required in this case.[63] If the mother or the child's father has not been deprived of parental rights and does not wish to give consent for adoption, that consent may, under legally prescribed conditions, be substituted by a court decision.[64]

54 Article 19(1), Convention on the Rights of the Child.
55 Committee on the Rights of the Child, *Concluding Observations on the Combined Third and Fourth Periodic Reports of India*, 2014, para. 42.
56 ECtHR Judgment of 13 February 2003, Case Odièvre v. France, application no. 42326/98, para. 45, hudoc.int.
57 Ibid.
58 Corte Costituzionale, Sentenza n. 425, 25 November 2005; Colcelli, "Anonymous Birth, Birth Registration," 4.
59 See also: Troiano, "Understanding and Redefining the Rationale of State Policies Allowing Anonymous Birth," 203.
60 Criminal Code of Republic of Croatia, Official Gazette, Nos. 125/2011, 144/2012, 56/2015, 61/2015, 101/2017, 118/2018, 126/2019, 84/2021, 114/2022, 114/2023, 36/2024.
61 Official Gazette, Nos. 103/2015, 98/2019, 47/2020, 49/2023, 156/2023.
62 Article 171 of the Family Act.
63 Article 188, para. 5 of the Family Act. See also: Hlača, "Pravo majke," 159.
64 Article 190, para. 1.

As for the argument of instigation to abandon a child, this argument can be viewed from two perspectives: a moral or philosophical one, and a legal one. The first seems completely unfounded. The existence of a baby hatch is just as encouraging of child abandonment as the existence of anonymous births in France, or the existence of other institutionalized modalities.[65] The argument that abandoning a child in the context of a baby hatch constitutes a criminal offense represents a shift into the criminal law domain. Article 37, paragraph 1 of the Criminal Code stipulates that whoever intentionally incites another to commit a criminal offense shall be punished as if he or she himself or herself has committed it. The key point is that the instigation must relate to a specific, concrete criminal act and a specific person, or a defined group of persons.[66] The argument that the existence of a baby hatch encourages the commission of a criminal offense is, therefore, entirely misguided.

3.3. Insufficiently Proven Effectiveness of Baby Hatches – Cost-Benefit Test

It is impossible to determine with certainty whether, and to what extent, baby hatches save human lives. A study conducted in Austria showed a "significant decrease in the number of police-reported neonaticide cases in Austria following the implementation of the anonymous delivery law in mid-2001" and a "possible connection of these two events."[67] Likewise, the number of abandoned children, as well as cases of infanticide, decreased after the introduction of baby hatches in Hamburg.[68] On the other hand, there are also studies that indicate the opposite.[69]

The argument that it has not been proven that baby hatches save lives[70] is, in fact, scientifically unsubstantiated. Moreover, some authors argue the opposite and even view baby hatches as a preventive measure to avoid infanticide.[71] Likewise, just as it is

65 Lorana Bartels, "Safe Haven Laws, Baby Hatches and Anonymous Hospital Birth: Examining Infant Abandonment, Neonaticide and Infanticide in Australia," *Criminal Law Journal* 36 (2012): 19–37, 34.

66 Željko Horvatić and Petar Novoselec, *Kazneno parvo: opći dio* (Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska akademija, 1999), 351; Berislav Pavišić and Petar Veić, *Komentar Kaznenog zakona* (Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska akademija, 1998), 125; Ivan Vukušić and Nina Mišić Radanović, "Pokušaj sudioništva u kaznenom pravu," *Hrvatski ljetopis za kazneno pravo i praksu* 22, no. 1 (2015): 95–123, 106.

67 Claudia M. Klier et al., "Is the Introduction of Anonymous Delivery Associated with a Reduction of High Neonaticide Rates in Austria? A Retrospective Study," *BJOG: An International Journal of Obstetrics & Gynaecology* 120, no. 4 (2013): 428–34, https://doi.org/10.1111/1471-0528.12099; see also: Christina Grylli et al., "Anonymous Birth Law Saves Babies – Optimization, Sustainability and Public Awareness," *Archives of Women's Mental Health* 19, no. 2 (2015): 291–97, https://doi.org/10.1007/s00737-015-0567-3.

68 Browne, Chou, and Whitfield, *Child Abandonment*, 22.

69 M. Orthofer and R. Orthofer, "Is the Introduction of Anonymous Delivery Associated with a Reduction of High Neonaticide Rates in Austria? A Retrospective Study," *BJOG: An International Journal of Obstetrics and Gynaecology* 120, no. 8 (2013): 1028, https://doi.org/10.1111/1471-0528.12260.

70 Troiano, "Understanding and Redefining of State Policies Allowing Anonymous Birth," 195. See: Tobias Bauer, "A Discussion of the Baby Hatch from the Viewpoint of a Child's Right to a Knowledge of His/Her Parentage: Perspectives from the German Debate," *Journal of Philosophy and Ethics in Health Care and Medicine*, no. 9 (2015): 31; ECtHR Judgment of 13 February 2003, Case Odièvre v. France, application no. 42326/98, para. 45, hudoc.int.

71 Stasiūnienė, Justickis, and Jasulaitis, "Newborn Murder," 115.

unknown, and cannot be known, how many lives – of both children and possibly mothers[72] – can be saved by a baby hatch, it is also impossible to determine how many lives would be destroyed by depriving individuals of their right to privacy due to ignorance of their own origins. More importantly, it is uncertain whether such deprivation would negatively affect the development of every child left in a baby hatch to such an extent that sacrificing someone's right to life for that knowledge would be justified.

In this regard, there are critiques that the issue should be considered not from an abstract, but from a concrete, statistical perspective. These critiques are based on the view that not all children left in a baby hatch would have been saved from a life-threatening situation if they had not been placed there. On the other hand, almost all such children would be deprived of the right to know information about their own origins, or, in conventional terms, their right to privacy. Therefore, according to these critiques, from an interpersonal perspective, the majority's right is sacrificed to save the right of a large minority.[73] The argument that, given the different ranking of the right to life and the right to privacy, such a sacrifice is acceptable, even if only one life is saved, could be rejected in this sense. In this context, it seems necessary to consider how many children's lives baby hatches would actually save and compare that number with the number of children who, due to baby hatches, have been deprived of their right to privacy.[74]

As much as the aforementioned considerations may make sense, in the context of insufficient evidence regarding the actual role of baby hatches in saving lives, the deprivation of the right to privacy for a larger number of children, and the risks posed to other institutions, they are essentially irrelevant from an intrapersonal as well as from an interpersonal perspective. From an intrapersonal viewpoint, the right to life takes precedence over or is above the right to privacy,[75] since the former implies the latter, as well as any other right, meaning that without the realization of the former, none of the others can exist.[76] From an interpersonal perspective, it seems indisputable that it would be acceptable to sacrifice the rights of many children to privacy to save the right to life of fewer children, simply because the right to life is superior to all other rights,[77] including the rights of all other persons.[78]

In this regard, Hadžimanović's conclusion that mothers should be allowed to consider whether they want to keep the child without any time pressure seems implausible, even though the note acknowledges that the child suffers if not provided with the love of a mother and father and if it does not become part of a family that can offer such love

---

72 Sylwia Olejarz, "Ethical Concerns Relating to Child Abandonment and Baby Hatches: The Case of Poland," *Journal of Philosophy and Ethics in Health Care and Medicine*, no. 11 (2017): 52.

73 Bauer, "Discussion of the Baby Hatch," 35; German Ethics Council, ed., *Anonymous Relinquishment of Infants: Tackling the Problem* (Berlin: German Ethics Council, 2009), https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/englisch/DER_Stn_AnonKind_Engl_online_Aufl2.pdf.

74 Bauer, "Discussion of the Baby Hatch," 37; Browne, Chou, and Whitfield, *Child Abandonment*, 17.

75 Bauer, "Discussion of the Baby Hatch," 34.

76 Troiano, "Understanding and Redefining of State Policies Allowing Anonymous Birth," 203; Mladenović, "Pravo na anonimni porođaj naspram prava deteta," 460.

77 Blažek and Prokeinová, "How to Provide a Legal Safe Harbor," 66.

78 Joint dissenting opinion of Judges Wildhaber et al., ECtHR Judgment of 13 February 2003, Case Odièvre v. France, application no. 42326/98, hudoc.int.

as soon as possible.[79] The best interest of the child is an impenetrable barrier protecting the child's right to grow up in a family founded through adoption, where they will receive the necessary love of a mother and father. This right cannot be overridden by the right of a woman, who may indefinitely hesitate whether to allow the realization of that child's right or not, especially considering that such a woman may be unable to make such a decision due to health or moral reasons.

4. Conclusion

Baby hatches are subject to criticism even from supporters of anonymous birth.[80] Indeed, they are not regulated by law, leaving a child in a baby hatch constitutes a criminal offense, and ultimately, that the institutions of anonymous and confidential birth are more acceptable from the perspective of protecting the health of both the mother and the child,[81] as well as from the perspective of safeguarding the child's right to know their origins.

In every discussion about anonymous birth, baby hatches, or any other form of care for anonymously abandoned children, a necessary condition for their justification is their institutionalization. This is the fundamental problem of baby hatches within the legal system of the Republic of Croatia. Legalization of baby hatches could be achieved through an appropriate amendment to the Criminal Code regarding the legal description of the criminal offense of Child Abandonment. An example can be found in Polish legislation and case law, according to which child abandonment includes leaving a child and ceasing to care for them without ensuring that another person takes responsibility for the child.[82]

The Committee on the Rights of the Child favors confidential birth. It considers the child's right to identity as the most important value to protect, despite the provision containing the limitation "as far as possible" and the fact, confirmed by the ECtHR, that all other rights derive from the right to life. Accordingly, the child's right to life is hierarchically superior to all other rights.

Here, we can mention Susan Ayres' reasoning that a woman in the given situation must have multiple options available "to do the right thing at the right time."[83] In this light, Judge Greve's concurring opinion is also relevant. This judge states that "it would be plainly inhumane to invoke human rights to force a woman in this situation to choose between abortion or a clandestine birth."[84]

Finally, the criticisms regarding the negative impact on other modalities that assist women wishing to give up their newborn children fail to consider that these very

79 Hadžimanović, "Confidential and Anonymous Birth," 130.

80 Troiano, "Understanding and Redefining of State Policies Allowing Anonymous Birth," 203.

81 Ibid.

82 Browne, Chou, and Whitfield, *Child Abandonment*, 30.

83 Sarah Ayres, "Kairos and Safe Havens: The Timing and Calamity of Unwanted Birth," *William & Mary Journal of Women and the Law* 15, no. 2 (2009): 289, https://ssrn.com/abstract=1356169; Govender, "An Ethico-Legal Case," 17. See also: Lemrová et al., "Anonymous Births," 38.

84 Concurring opinion of Judge Greve, ECtHR Judgment of 13 February 2003, Case Odièvre v. France, application no. 42326/98, hudoc.int.

modalities may represent too great a challenge for some women. Some may hesitate to use institutionalized options out of fear that their identity might still be revealed.[85] In countries where anonymous birth is regulated, there is always a risk that anonymity may be compromised by medical or other staff, or, for example, by visitors.[86] An unavoidable factor that might lead women to avoid other modalities is the fear of social stigma,[87] criminal prosecution,[88] or family members.[89]

Moreover, there are factors of mental, moral, and intellectual maturity. Discussions generally focus on mature and competent individuals, but often overlook those who are simply not intellectually capable of engaging in procedural legal actions required by certain modalities. Also, as noted by Asai and Ishimoto, there are individuals who, whether out of fear or selfishness, do not wish to communicate with either their relatives or the competent institutions, as well as those who are unable to do so for various reasons.[90] They conclude that "we should consider the continuation of baby hatches with such realities in mind."[91]

At this point, it seems appropriate to highlight the concurring opinion of Judges Ress and Kūris, as harsh as it may sound, according to which "persons who seek disclosure at any price, even against the express will of their natural mother, must ask themselves whether they would have been born had it not been for the right to give birth anonymously."[92]

Such a view confirms the primacy of the right to life. Ultimately, the situation in which a woman leaves a child in a baby hatch or enters the anonymous birth system is undoubtedly the result of circumstances indicating that the quality of the child's life would have been questionable, even if the child had been kept. Furthermore, it is likely that, in the case of adoption, such a child will experience all aspects of parenthood within their new family, where their quality of life will be ensured in every respect. This was also stated in the case of *Odièvre v. France*, where the ECtHR held that Ms. Odièvre "has parental ties with her adoptive parents and a prospective interest in their property and estate."[93] Therefore, one should not assume that, in these cases, quality of life would be sacrificed at the expense of the right to life.[94] The right to knowledge of one's origins would be sacrificed for the protection of the right to a life of full quality. Ultimately, nothing prevents a woman from leaving some information about herself when leaving the child, which would one day enable the child to discover their own identity.

Against the backdrop of these competing interests, it is indisputable that the paramount legal objective is the protection of the child's best interests, which necessarily

85 E.g., Lemrová et al., "Anonymous Births," 37.
86 Olejarz, "Ethical Concerns," 50.
87 Ibid., 51.
88 E.g., Baqutayan et al., "Should We Maintain Baby Hatches."
89 See: Rosenberg, "Illegality of Baby Safes," 207.
90 Asai and Ishimoto, "Should We Maintain Baby Hatches in Our Society?," 7.
91 Ibid.
92 Concurring opinion of Judges Ress and Kūris, ECtHR Judgment of 13 February 2003, Case Odièvre v. France, application no. 42326/98.
93 ECtHR Judgment of 13 February 2003, Case Odièvre v. France, application no. 42326/98, para. 56.
94 Olejarz, "Ethical Concerns," 47.

encompasses the safeguarding of the child's life.[95] In this framework, while striving to identify an optimal solution that balances the interests of both the child and the parents, baby hatch facilities serve as a practical instrument toward the realization of the highest principle – the protection of the child's life.

References

Asai, Atsushi, and Hiroko Ishimoto. "Should We Maintain Baby Hatches in Our Society?." *BMC Medical Ethics* 14, no. 9 (2013): 1–7. https://doi.org/10.1186/1472-6939-14-9.

Ayres, Sarah. "Kairos and Safe Havens: The Timing and Calamity of Unwanted Birth." *William & Mary Journal of Women and the Law* 15, no. 2 (2009): 227–89. https://ssrn.com/abstract=1356169.

Baqutayan, Shadiya Mohamed, Salwa Ahmad Rafee, Aspah Aini Ishak, Muhammad Rohaizad Razali, and Nor Baizura Mohd Noordin. "Should We Maintain Baby Hatches in Our Society? Baby Hatch Policy in Malaysia." *International Journal of Academic Research in Business and Social Sciences* 12, no. 11 (2022): 3073–88. https://doi.org/10.6007/IJARBSS/v12-i11/15032.

Bartels, Lorana. "Safe Haven Laws, Baby Hatches and Anonymous Hospital Birth: Examining Infant Abandonment, Neonaticide and Infanticide in Australia." *Criminal Law Journal* 36 (2012): 19–37.

Bauer, Tobias. "A Discussion of the Baby Hatch from the Viewpoint of a Child's Right to a Knowledge of His/Her Parentage: Perspectives from the German Debate." *Journal of Philosophy and Ethics in Health Care and Medicine*, no. 9 (2015): 31–43.

Blažek, Rodovan, and Margita Prokeinová. "How to Provide a Legal Safe Harbor for Mothers of Unwanted Newborns." *Issues in Law & Medicine* 32, no. 1 (2017): 53–70.

Browne, Kevin, Shihning Chou, and Kate Whitfield. *Child Abandonment and Its Prevention in Europe*. Nottingham: The University of Nottingham, 2012.

Colcelli, Valentina. "Anonymous Birth, Birth Registration and the Child's Right to Know Their Origins in the Italian Legal System: A Short Comment." *Journal of Civil & Legal Sciences* 1, no. 2 (2013): 101. https://doi.org/10.4172/2169-0170.1000101.

European Court of Human Rights. *Guide on Case-Law of the European Convention on Human Rights: Rights of the Child*. Strasbourg: Council of Europe, 2025. Accessed February 23, 2026. https://ks.echr.coe.int/documents/d/echr-ks/guide_rights_of_the_child_eng.

European Court of Human Rights. *Guide to the Case-Law of the European Court of Human Rights: Data Protection*. Strasbourg: Council of Europe, 2020.

German Ethics Council, ed. *Anonymous Relinquishment of Infants: Tackling the Problem*. Berlin: German Ethics Council, 2009. https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/englisch/DER_Stn_AnonKind_Engl_online_Aufl2.pdf.

Govender, Kurium. "An Ethico-Legal Case for Baby Hatches in South Africa." MSc diss., University of the Witwatersrand, Johannesburg, 2021. https://wiredspace.wits.ac.za/items/12cc9eee-b0c2-4e92-ab95-459fe5c03e50.

Grylli, Christina, Ian Brockington, Christian Fiala, Mercedes Huscsava, Thomas Waldhoer, and C.M. Klier. "Anonymous Birth Law Saves Babies – Optimization, Sustainability and Public Awareness." *Archives of Women's Mental Health* 19, no. 2 (2015): 291–97. https://doi.org/10.1007/s00737-015-0567-3.

[95] Nataša Lucić, "Anonimni porod – treba li nam zakonsko uređenje?," *Pravni vjesnik: časopis za pravne i društvene znanosti Pravnog fakulteta Sveučilišta J.J. Strossmayera u Osijeku* 41, no. 4 (2025): 45, https://doi.org/10.25234/pv/37480.

Hadžimanović, Nataša. "Confidential and Anonymous Birth in National Laws: Useful and Compatible with the UN Convention on the Rights of the Child?." *Comparazione e diritto civile* (2018): 119–43. https://www.comparazionedirittocivile.it/data/uploads/archivio-volumi/201801.pdf.

Hlača, Nenad. "Pravo majke na anonimnost poroda – 'L'accouchement sous X – Porod pod X'." *Gynaecologia et Perinatologia* 16, no. 3 (2007): 157–60.

Horvatić, Željko, and Petar Novoselec. *Kazneno pravo: Opći dio*. Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska akademija, 1999.

Initiative for Reproductive Health Information (IRHI). "Anonymous Birth." Accessed October 9, 2025. https://anonymegeburt.at/anonymous-birth.

Klier, Claudia M., Chryssa Grylli, Sabine Amon, Christian Fiala, Ghitta WeizmannHenelius, Sandi L. Pruitt, and Hanna Putkonen. "Is the Introduction of Anonymous Delivery Associated with a Reduction of High Neonaticide Rates in Austria? A Retrospective Study." *BJOG: An International Journal of Obstetrics & Gynaecology* 120, no. 4 (2013): 428–34. https://doi.org/10.1111/1471-0528.12099.

Lemrová, Adéla, Ivana Olecká, Ester Hladíková, and Kateřina Ivanová. "Anonymous Births: A Conflict of Three Rights – Which Prevails?." *Social Pathology and Prevention* 7, no. 2 (2022): 35–46. https://doi.org/10.25142/spp.2022.003.

Lucić, Nataša. "Anonimni porod – treba li nam zakonsko uređenje?." *Pravni vjesnik: časopis za pravne i društvene znanosti Pravnog fakulteta Sveučilišta J.J. Strossmayera u Osijeku* 41, no. 4 (2025): 25–50. https://doi.org/10.25234/pv/37480.

Mladenović, Tamara. "Pravo na anonimni porođaj naspram prava deteta na identitet." *Pravni zapisi* 12, no. 2 (2021): 443–63. https://doi.org/10.5937/pravzap0-34192.

O'Donovan, Katherine. "'Real' Mothers for Abandoned Children." *Law & Society Review* 36, no. 2 (2002): 347–78.

Olejarz, Sylwia. "Ethical Concerns Relating to Child Abandonment and Baby Hatches: The Case of Poland." *Journal of Philosophy and Ethics in Health Care and Medicine*, no. 11 (2017): 41–61.

Orthofer, M., and R. Orthofer. "Is the Introduction of Anonymous Delivery Associated with a Reduction of High Neonaticide Rates in Austria? A Retrospective Study." *BJOG: An International Journal of Obstetrics and Gynaecology* 120, no. 8 (2013): 1028. https://doi.org/10.1111/1471-0528.12260.

Pavišić, Berislav, and Petar Veić. *Komentar Kaznenog zakona*. Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske, Policijska akademija, 1998.

Praduroux, Sabrina. "The Right to Know One's Genetic Origins: A Right in Need of Regulation." *Italian Law Journal* 7, no. 2 (2021): 803–20. https://dx.doi.org/10.23815/2421-2156.ITALJ.

Preložnjak, Barbara. "Modern Challenges in the Implementation of the Child's Right to Know His Origin." *EU and Comparative Law Issues and Challenges Series (ECLIC)* 4 (2020): 1175–203. https://doi.org/10.25234/eclic/11944.

Rosenberg, Whitney. "The Illegality of Baby Safes as a Hindrance to Women Who Want to Relinquish Their Parental Rights." *Athens Journal of Law* 1, no. 4 (2015): 201–12. https://doi.org/10.30958/ajl.1-4-1.

Stasiūnienė, Jurgita, Viktoras Justickis, and Algimantas Jasulaitis. "Newborn Murder and Its Legal Prevention." *Health Policy and Management* 1, no. 8 (2015): 91–119. https://doi.org/10.13165/SPV-15-1-8-05.

Troiano, Stefano. "Understanding and Redefining the Rationale of State Policies Allowing Anonymous Birth: A Difficult Balance Between Conflicting Interests." *International Journal of Jurisprudence of the Family* 4 (2013): 177–204. https://ssrn.com/abstract=322394.

United Nations. *Legislative History of the Convention on the Rights of the Child*. New York–Geneva: UN, 2007. Accessed October 9, 2025. https://digitallibrary.un.org/record/602462?v=pdf.

Vukušić, Ivan, and Nina Mišić Radanović. "Pokušaj sudioništva u kaznenom pravu." *Hrvatski ljetopis za kazneno pravo i praksu* 22, no. 1 (2015): 95–123.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 103–116
https://doi.org/10.31743/recl.19198
Received: 10 November 2025 | Accepted: 26 February 2026 | Published: 31 March 2026

The Concept of Cyber Resilience in the European Union Law

Grażyna Szpor

PhD habil., Professor, Department of Informatics Law, Faculty of Law and Administration, Cardinal Stefan Wyszyński University in Warsaw; correspondence address: Wóycickiego 1/3 Street, building 17, 01–938 Warsaw, Poland; e-mail: g.szpor@uksw.edu.pl
https://orcid.org/0000-0002-3264-9360

Abstract: The legal framework for digital transformation in the European Union is being supplemented by further acts that should enable it to meet current challenges while respecting EU values and principles redefined in the context of cyberspace. An example is Regulation 2024/2847 on horizontal cybersecurity requirements (Cyber Resilience Act). It does not define the term used in the abbreviated title. The relationship between cyber resilience and cybersecurity, and their place within the conceptual framework of digital transformation, remains unclear. This article aims to identify terminological issues that require doctrinal agreement, to consider the possibilities for achieving this, and to propose solutions. An analysis of how the purpose of the act is reflected in its title, definitions, scope, structure and initial stage of application was carried out using a legal-dogmatic method, including a systemic approach. It confirmed the verified hypotheses about the underestimation of the importance of short titles of acts in EU legislative processes and the untapped potential of the concept of cyber resilience in increasing the consistency and transparency of law, which is essential for its effectiveness. The result is a proposal to amend EU legislative drafting rules on short titles and to adopt a general definition of cyber resilience as a higher-order concept capable of integrating scattered sectoral regulations and performing an organizing function for digital transformation processes in legal doctrine.

Keywords: EU law, digital transformation, cybersecurity, cyber resilience, definition

1. Introduction

The role of law in digital transformation is to remove barriers to development, while also establishing restrictions deemed necessary to protect fundamental human rights and the public interest. Legal instruments for cybersecurity protection initially focused on incident response. However, due to the rapid increase in cyberattacks, including cyber operations conducted by hostile states, legislators have shifted their approach from reactive to proactive, encompassing broader diagnosis and threat reduction.[1]

In addition to changes in "sectoral" regulations, "horizontal" solutions have also emerged. An example is the Cyber Resilience Act (2024/2847)[2] (hereinafter: CRA), which

[1] Bolesław Szafrański, ed., *Cyberbezpieczeństwo: redefinicja zagrożeń* [Cybersecurity: Redefining Threats] (Warsaw: Wojskowa Akademia Techniczna, 2023).

[2] Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20 November 2024) (hereinafter: CRA).

ISSN 2545-384X (Online)

establishes horizontal cybersecurity requirements for products with digital elements.[3] The term "cyber resilience" has no legal definition, so its meaning needs to be verified.

Using a legal-dogmatic method, including systemic interpretation, the following parts of this article analyze: the compliance of the title of the regulation with EU legislative principles; the contexts in which the term cyber resilience appears (in the regulation and in other acts); the division of the protection of the cyber resilience of products with digital elements between the CRA and other acts; the links between the CRA glossary and the conceptual framework of digital transformation; the addressees of new obligations in the phase of partial application of the CRA.

In existing interdisciplinary research focusing on many aspects of cyber resilience, the meaning of this term is interpreted differently,[4] prompting attempts at harmonization. Assessments of legalization should also take into account the criteria of consistency and transparency, whose importance for the effectiveness of law is highlighted by new EU initiatives such as the Omnibus.[5]

2. Title and Purpose of the Cyber Resilience Act

The titles of EU legislative acts, including regulations, are determined by the Annex 1 of the *Joint Handbook for the Presentation and Drafting of Acts Subject to the Ordinary Legislative Procedure*,[6] adopted in October 2023 to facilitate cooperation between the European Parliament, the Council, and the Commission. It is not binding on the political bodies involved in the legislative process, but it does provide a "toolbox" that significantly impacts the formal aspects of new acts.

According to the guidelines contained in this document, the title of the act should signal its content in as concise and complete a manner as possible, without misleading the recipient as to the content of the normative part. The full title of the act may be followed by a short title. Therefore, the title Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020, and Directive (EU) 2020/1828 (Cyber Resilience Act)[7] is generally in line with EU legislative drafting principles. However, it is not clear whether this also applies to the short title.

---

3 In addition, it amends two previous regulations: 168/2013 and 2019/1020, as well as Directive 2020/1828, and also contains a number of provisions referring to previously adopted EU acts.

4 Igor Linkov and Alexander Kott, "Fundamental Concepts of Cyber Resilience: Introduction and Overview," in *Cyber Resilience of Systems and Networks: Risk, Systems and Decisions*, eds. Alexander Kott and Igor Linkov (Cham: Springer, 2019), 1–25, https://doi.org/10.1007/978-3-319-77492-3_1.

5 European Commission, *Omnibus I*, COM(2025) 80 final (Brussels: European Commission, 26 February 2025); European Commission, *Omnibus II*, COM(2025) 84 final (Brussels: European Commission, 26 February 2025).

6 European Parliament, Council of the European Union, and European Commission, *Joint Handbook for the Presentation and Drafting of Acts Subject to the Ordinary Legislative Procedure*, October 2023 ed., Annex I: *Joint Practical Guide of the European Parliament, the Council and the Commission for Persons Involved in the Drafting of European Union Legislation*, pt. 8, pp. 18–20, https://www.consilium.europa.eu/media/67390/joint_handbook_en_01-october-2023_clean_def_final.pdf.

7 CRA (OJ L, 2024/2847, 20 November 2024).

The guidelines assume that short titles in Union law, where acts are identified by letters and numbers (e.g., (EU) 2025/1234), are less useful than in systems that do not use such a numbering system. It is emphasized that

> 8.4. In certain cases, however, a short title has come to be used in practice (…). Despite the fact that it may seem a simple solution, referring to acts by a short title creates risks for the accuracy and coherence of legal acts of the Union. This method should therefore only be used in specific cases where it significantly aids the reader's understanding.
>
> 8.5. The creation of a short title when an act is adopted by adding it after the title of the act should be avoided, since it only renders the title more cumbersome (…). While the risks outlined in point 8.4 must always be borne in mind, it is possible to refer to an act by using a short title in order to make it easier to understand the act in which the reference is made. In this case, the short title chosen will have to appear in brackets in the body of the text of the act in which the reference is made, like any other abbreviation.[8]

The main regulations and directives on digital transformation often have abbreviated titles.[9] At the same time, in scientific publications and public discourse, these abbreviated titles are widely used and sometimes replaced by even more informal abbreviations, mainly acronyms of elements of the title in English (NIS, CRA) or the national language. For example, in Poland, the commonly used term is not "General Data Protection Regulation" or GDPR,[10] but RODO. When applying the law, it is usually necessary to address the dispersion of many acts related to a specific administrative matter. The use of numbers makes the texts of the grounds for judgments and decisions incomprehensible to the recipient. This justifies the recommendation to amend the EU guidelines by abandoning the "uniqueness" of placing the abbreviated version of the title of a regulation or directive at the end.

A separate issue is the content of short titles and their placement in the provisions to which they refer. For example, in the CRA, the term "cyber resilience" appears in the title, in five recitals of the preamble and only once outside the preamble, in Article 33(2) (cyber resilience regulatory sandboxes). Recital (1), which states that cybersecurity is one of the most serious challenges facing the Union, seems to be of fundamental importance for the adoption of the short title:

> In the coming years, the number and variety of devices connected to the internet will grow rapidly. Cyberattacks are a matter of public interest because they have a decisive impact not only on the Union's economy, but also on the democratic system, consumer safety and health. It is therefore necessary to strengthen the Union's approach to cybersecurity, address the issue

---

8 European Parliament, Council of the European Union, and European Commission, *Joint Handbook for the Presentation and Drafting of Acts Subject to the Ordinary Legislative Procedure*, pts. 8.4–8.5, p. 19, https://www.consilium.europa.eu/media/67390/joint_handbook_en_01-october-2023_clean_def_final.pdf.

9 For example: Data Act, Data Governance Act, Digital Service Act, Artificial Intelligence Act, Interoperable Europe Act, Cybersecurity Act, Cybersolidarity Act. When considering the introduction of the prefix "cyber" into the titles of acts, it should be noted that in English, this prefix already appears in over 600 words.

10 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 May 2016), 1–88.

of cyber resilience at Union level and improve the functioning of the internal market by establishing a single regulatory framework covering essential cybersecurity requirements for the placing of products with digital elements on the Union market.

The short titles of other EU acts refer to legally protected values such as security and solidarity, which are redefined in the context of cyberspace,[11] e.g., in the Cybersecurity Act[12] or the Cyber Solidarity Act.[13] This raises the question of whether the term "cyber resilience" used in the short title of Regulation 2024/2847, which refers to products with digital elements, can also be treated as a systemic category linking many regulatory regimes and, more broadly, whether the reference to protected values[14] should not be the first choice and become good practice in the formulation of short titles.

3. Definitions

The term "cyber resilience," which appears in the title of Regulation 2024/2847, has not yet been given a legal definition, nor does the CRA contain one. However, the lack of a legal definition does not mean that there is no normative content – on the contrary, it points to the need for doctrinal reconstruction.[15]

Achieving clarity of the term is undoubtedly hampered by the multitude of contexts in which it is used. In the CRA itself, the preamble contains the phrases: "cyber resilience of products with digital elements" (108), "cyber resilience at global level" (123), "cyber resilience at EU level" (1), "cyber resilience of economic operators" (128), "cyber resilience

11 The axiological aspects of digital transformation are further specified in the joint "European Declaration on Digital Rights and Principles for the Digital Decade" proclaimed by the European Parliament, the Council, and the European Commission. European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01 (OJ C 23, 23 January 2023), 1–7; Grażyna Szpor, "Prawa jednostki i wspólnoty w Cyfrowej Dekadzie" [Rights of Individuals and Communities in the Digital Decade], in *W trosce o dobro wspólnoty i jednostki – zagadnienia administracyjnoprawne. Księga jubileuszowa dedykowana Profesor Zofii Duniewskiej* [For the Good of the Community and the Individual: Administrative and Legal Issues. Jubilee Book Dedicated to Professor Zofia Duniewska], eds. Barbara Jaworska-Dębska et al. (Warsaw: Wolters Kluwer, 2024), LEX/el.

12 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7 June 2019), 15–69.

13 Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) (OJ L, 2025/38, 15 January 2025).

14 Pier Giorgio Chiara, "Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?," *European Journal of Risk Regulation* 16, no. 2 (2025): 469–84, https://doi.org/10.1017/err.2025.9.

15 Fredrik Björck et al. "Cyber Resilience – Fundamentals for a Definition," in *New Contributions in Information Systems and Technologies*, vol. 1, eds. Alvaro Rocha et al. (Cham: Springer, 2015), 311–16, https://doi.org/10.1007/978-3-319-16486-1_31; Kjell Hausken, "Cyber Resilience in Firms, Organizations and Societies," *Internet of Things* 11 (2020): 100204, https://doi.org/10.1016/j.iot.2020.100204; Wojciech R. Wiewiórowski. "Europejskie roumienie cyberodporności" [European Understanding of Cyber Resilience], in *Internet. Cyberodporność. Cyber Resilience*, eds. Agnieszka Gryszczyńska, Grażyna Szpor, and Wojciech R. Wiewiórowski (Warsaw: C.H. Beck, 2025), 95–104.

of artificial intelligence systems" (51), and in Article 33(2) "cyber resilience regulatory sandboxes."[16]

This may lead to the formulation of many contextual definitions of cyber resilience, but the frequent co-application of several acts limits their usefulness. It is also possible – omitting the prefix "cyber" at the beginning – to refer to the legal definitions of the term resilience, which, however, are also contextual in nature. EU Regulation 2021/2041 states that "resilience" means the ability to cope with economic, social, and environmental shocks or persistent structural changes in a fair, sustainable, and inclusive manner.[17] In contrast, Directive (EU) 2022/2557 of the European Parliament and of the Council defines resilience as the ability to "prevent, protect against, respond to, resist, mitigate, and absorb an incident, and adapt and recover from an incident."[18] The literature emphasizes that achieving an acceptable level of resilience requires preventive measures to identify threats before they cause adverse effects,[19] which aligns with the nearly 100 uses of the terms "threat" and "cyber threat" in the NIS2 Directive.[20] In general terms, resilience is the ability of an entity to continue achieving its intended objectives despite cyber incidents,[21] which includes the ability to detect and counter threats, respond quickly to undesirable events, and maintain business continuity.[22]

Cyber resilience, as shown by the results of multidisciplinary research, is considered in the contexts of IT systems, critical infrastructure, business processes, organizations, societies, nation states, the EU, and the global community. If we cannot agree on a single, universal answer to the question of how to understand cyber resilience, then the appearance of this term in law and official documents should be accompanied by explanations of its meaning in a given context, to reduce doubts and ensure uniformity in the application of law and the performance of public tasks. Integrating the non-contradictory elements of the analysis, carried out using the legal-dogmatic method, it can be concluded that:

> Cyber resilience is the ability to cope with security challenges related to the digital transformation. As a legal concept, it refers to products with digital elements as well as social and economic processes, information and political-organisational systems. It includes detecting and

16 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20 November 2024).

17 Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility (OJ L 57, 18 February 2021), 17–75, Article 2(5).

18 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333/164, 27 December 2022).

19 Sławomir Dygnatowski, "Cyber Security as a Foundation for the Security of Critical Infrastructure in the Context of Modern Threats," *Journal of Konbin* 50, no. 4 (2020): 317, https://doi.org/10.2478/jok-2020-0089.

20 Szafrański, ed., *Cyberbezpieczeństwo*, 295–306.

21 A related term is cyberworthiness, which is a measure of a system's resilience to cyber incidents (cyber-attacks) and can be applied to software and hardware components. "Cyber Resilience," Wikipedia, https://en.wikipedia.org/wiki/Cyber_resilience.

22 Dominika Skoczylas, "Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń" [Strengthening the European Union's Cybersecurity Capabilities: Cyber Solidarity in the Context of Cyber Threats], *Europejski Przegląd Sądowy*, no. 12 (2024): 39–44.

> reducing threats, responding to undesirable events and achieving objectives despite various disruptions: intentional and accidental, natural and man-made.[23]

Such a reconstruction allows us to see that cyber resilience is not limited to a single area of regulation, but can integrate across areas.

For the purposes of the CRA, 51 definitions contained in Article 3 are used, including 15 definitions referring to seven previous EU acts: Regulation 2019/881 (cybersecurity, cyber threat), Directive 2022/2555 (incident, near miss, CSIRT designated as coordinator), Regulation 2016/679 (personal data), Regulation 2019/1020 (Union harmonization legislation,[24] market surveillance authority, recall, withdrawal), Regulation (EU) No 1025/2012 (international standard, European standard, harmonized standard), Regulation (EC) No 765/2008 (conformity assessment body), and Recommendation 2003/361/EC (micro-enterprises, small enterprises, and medium-sized enterprises). Article 3 also contains definitions that refer in part to the CRA itself (point 29 – notified body to Article 43) and its annexes (point 20 – support period, point 27 – conformity assessment, point 31 – CE marking).

The extensive system of references confirms that the CRA does not create an autonomous regime but integrates existing elements into a new normative framework. From the perspective of legal theory, this means that cyber resilience functions as a systemic category, organizing the relationships between dispersed instruments of EU law.

In addition, 37 new definitions apply to the CRA, which can be divided into three groups: (1) definitions relating to products and their components, (2) subjective definitions, and (3) objective definitions related to placing on the market and risks in cyberspace.

The first group includes the term contained in the title of the act and the cascading terms that make up its definition, as well as those used in their explanation. Article 3(1) of the CRA states that "product with digital elements" means a software or hardware product and its remote data processing solutions (including software or hardware components that are being placed on the market separately). "Remote data processing" means the processing of data at a distance, for the purposes of which the software has been designed and developed by the manufacturer or under the manufacturer's responsibility, and the absence of which would prevent the product with digital elements from performing one of its functions (point 2). "Software" means a part of an electronic information system, which consists of computer code (point 4).[25] "Electronic information sys-

---

[23] Grażyna Szpor, "Introduction," in *Internet. Cyberodporność. Cyber Resilience*, eds. Agnieszka Gryszczyńska, Grażyna Szpor, and Wojciech R. Wiewiórowski (Warsaw: C.H. Beck, 2025), LXI and publications cited therein.

[24] CRA Article 3(32) contains an exception to the rule adopted for cross-references, "x means x as defined in...," and states: "Union harmonisation legislation" means the Union provisions listed in Annex I to Regulation (EU) 2019/1020 and any other Union provisions harmonizing the conditions for the marketing of products to which that Regulation applies.

[25] In addition to the definition of software in Article 3(48) of the CRA, "free and open-source software" is also defined.

tem" means a system, including electrical or electronic equipment, capable of processing, storing, or transmitting digital data (point 7). "Hardware" means a physical electronic information system or its parts capable of processing, storing or transmitting digital data (point 5). "Component" means software or equipment intended for integration into an electronic information system (point 6). Integration may take the form of a "logical connection" (point 8), a "physical connection" (point 9), or an "indirect connection" (point 10), whereby any device that is connected to a network and serves as an entry point to that network is referred to as an "end point" (point 11). The structure of this part of the glossary exemplifies careful adherence to the principles of legislative technique and a desire to ensure both internal and external terminological consistency.

The second group clarifies, in the context of the CRA, the meaning of terms relating to entities, such as: economic operator (12), manufacturer (13), authorized representative (15), importer (16), distributor (17), consumer (18), and notifying authority (26) – already widely used in law. With regard to this group of terms, despite their definition, conflicts may arise when several acts are applied simultaneously. An exception is the original term "open-source software steward,' which does not appear previously in EU law and is broadly defined as:

> [A] legal person other than the manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products (point 14).[26]

The third group of defined terms covers substantive aspects: "placing on the market" (21), "making available on the market" (22), and distinguishes between "intended purpose" (23), "reasonably foreseeable use" (24),[27] and "reasonably foreseeable misuse" (25), which, by overcoming the previous vagueness of the scope, may facilitate the achievement of the objectives of the act. This group also includes the terms "cybersecurity risk" (37) and "significant cybersecurity risk" (38). On eur-lex.pl, "cybersecurity risk" is translated into Polish as "ryzyko w cyberprzestrzeni" (risk in cyberspace). From a Polish perspective, this raises doubts because cyberspace has a legal definition unrelated to incidents,[28] and, for example, a corrigendum was made in Commission Delegated Regulation (EU) 2024/1366,[29] changing the Polish text from "ryzyko w cyber-

[26] On the CRA's attempt to balance cybersecurity obligations with the development of open-source solutions, see: Mattis van 't Schip, "The Cyber Resilience Act and Open-Source Software: A Fine Balancing Act," *Journal of Intellectual Property, Information Technology and E-Commerce Law* 16, no. 1 (2025) 73–87.

[27] An application that is not necessarily the intended purpose specified by the manufacturer in the user manual, promotional or sales materials and statements, as well as in technical documentation, but which is most likely to result from reasonably foreseeable human behavior, technical operations or interactions (which may refer to so-called "dual-use items") – civil and military.

[28] Act on Martial Law and the Powers of the Commander-in-Chief of the Armed Forces and the Principles of his Subordination to the Constitutional Authorities of the Republic of Poland (i.e., Journal of Laws 2025, item 504).

[29] Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, C/2024/1383 (OJ L, 2024/1366, 24 May 2024); Rectificatif au règlement délégué (UE) 2024/1366 de la Commission du 11 mars 2024 complétant le règlement

przestrzeni" (risk in cyberspace) to "ryzyko cyberbezpieczeństwa" (cybersecurity risk). However, it is worth considering the definition of cyberspace and the risks associated with it in EU law.[30]

An analysis of the 51 definitions contained in Article 3 of the CRA shows that the legislator is building a coherent, logical conceptual structure and "operationalizing" security requirements, but does not exhaust the ontological scope of cyber resilience. However, the comparison also shows that the cyber resilience of products with digital elements is built on the current conceptual framework of digital transformation and, on the other hand, this framework is specified for the future in a broader sense than just those products.

4. Scope and Structure of the Cyber Resilience Act

The legal basis for digital transformation in the European Union, including cybersecurity, is typically shaped by the adoption of prospective acts (strategies, plans) first, followed by a gradual transition to directives, creating cross-border information links and regulations. Such phases can also be distinguished in relation to cyber resilience. In the current phase, in which several EU directives, regulations and decisions already refer to resilience in cyberspace, the CRA is sometimes referred to as an instrument that closes the system, ensuring that hardware and software are placed on the market with as few vulnerabilities as possible, that manufacturers provide security updates throughout the product lifecycle, and that information on safe use is understandable and easily accessible.[31]

From a legal perspective, this closing function is demonstrated not only by the cross-referenced definitions discussed above. It is also confirmed by the reference to other regulations in the extensive preamble, which contains 130 recitals,[32] as well as numerous specific exemptions in the general provisions relating to the scope of the CRA, which are important for harmonious cooperation and the avoidance of conflicts of competence in the application of the law.[33]

Regulations of the European Parliament and of the Council are binding in their entirety and directly applicable in all Member States, as provided for in Article 71(2) of the CRA. The fact that "an act is binding in its entirety" excludes, as emphasized in doctrinal

(UE) 2019/943 du Parlement européen et du Conseil en établissant un code de réseau sur des règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité (OJ L, 2024/90558, 16 September 2024).

30 See: Grzegorz Pilarski, "Tackling Cyberspace Threats: The International Approach," *Security and Defence Quarterly* 12, no. 3 (2016): 100–17, https://doi.org/10.35467/sdq/103238.

31 Krzysztof Silicki, "Cyberodporność wspierana przepisami prawa UE: akt o cyberodporności (CRA) i dyrektywa NIS 2" [Cyber Resilience Supported by EU Laws: Cyber Resilience Act and NIS2 Directive], in *Internet. Cyberodporność. Cyber Resilience*, 105–18.

32 See preamble, recitals 117 and 118, and recital 46 et seq.

33 Grażyna Szpor and Paweł Hajduk, "Współdziałanie w egzekwowaniu przepisów z zakresu cyberbezpieczeństwa" [Cooperation in the Enforcement of Cybersecurity Regulations], in *Cyberbezpieczeństwo. Współpraca versus konfrontacja informacyjna* [Cybersecurity: Cooperation versus Informational Confrontation] ed. Bolesław Szafrański (Warsaw: Wojskowa Akademia Techniczna, 2025), 297–307.

interpretation, its "selective or incomplete" application.[34] However, the EU legislator itself establishes in many regulations the possibility of limiting or excluding the application of certain provisions in EU or national law, or of the national legislator shaping certain issues differently.[35]

The CRA applies – as provided for in Article 2(1), meticulously using the terms defined in Article 2 – "to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network." However, as many as seven subsequent paragraphs of this article (2–8) precisely define the limits of application, first excluding in paragraphs 2–4 such products with digital elements to which the three previous EU regulations (2017/745, 2017/746, 2019/2144), products certified in accordance with Regulation (EU) 2018/1139, and products covered by Directive 2014/90. The fifth point provides for the possibility of limiting or excluding the application of the CRA to products with digital elements covered by other EU legislation establishing requirements relating to all or certain types of risk, if this is consistent with the general regulatory framework and sectoral legislation provides the same or a higher level of protection than the CRA. In this regard, the Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement the CRA by specifying whether such a restriction or exemption is necessary and to what extent. Further exemptions from the application of the CRA concern certain spare parts made available on the market (6), as well as products developed or modified exclusively for national security or defense purposes (7), and specifically designed for processing classified information (7). Finally, it is stipulated that the obligations laid down in the CRA "shall not entail the supply of information the disclosure would be contrary to the essential interests of national security, public security or defence" (8).

The analysis shows, on the one hand, a complex network of interconnections and, on the other, a diversity of methods and criteria for limiting the scope of the new EU act. Cyber resilience is included in the CRA as a set of common requirements relating to the market for products with digital elements, which are specified in other EU and national legislation and technical standards. This horizontal approach should, therefore, not interfere with the adaptation of the protection of individual product categories with digital elements to different threats and risk levels. Therefore, the CRA is not a comprehensive regulation for the cyber resilience of products with digital elements, but it is a leading act that brings together standards for such products, which are scattered across many acts.

5. Structure of the CRA and Dates of Entry into Force and Application

The structure of the CRA – comprising general provisions, obligations of economic operators, conformity assessment, notification of bodies, market surveillance, and transitional

[34] Tomasz Jaroszyński, *Rozporządzenie Unii Europejskiej jako składnik systemu prawa obowiązującego w Polsce* [European Union Regulation as a Component of the Legal System in Force in Poland] (Warsaw 2011), LEX/el.

[35] Michał Czerniawski, "Art. 93," in *Akt o usługach cyfrowych. Komentarz*, eds. Dominik Lubasz and Monika Namysłowska (Warsaw: Wolters Kluwer, 2024), SIP LEX.

provisions[36] – corresponds to the classic model of a harmonization regulation. Transparency is enhanced by the transfer of specific issues to eight extensive annexes.

Digital economy operators implementing the numerous requirements established by the Cybersecurity Act and resulting from national implementations of the NIS 2 Directive should have stronger guarantees than before that the hardware and software on which their information infrastructure is built meet equivalent requirements throughout the EU. Various aspects of these changes have already been the subject of detailed consideration and assessment, including critical comments on the difficulties of rapidly implementing many new obligations.[37] In this context, it should be noted that the dates of publication, entry into force, and application should be permanent elements of the dogmatic analysis of a legal act. They can also be considered more broadly, in the context of legal culture, which is important for achieving the desired consistency, functionality, transparency, and certainty of the law.[38]

The CRA – as provided for in Article 71 – enters into force on the twentieth day following its publication in the Official Journal of the European Union (L 2024/2847), which took place on November 20, 2024, i.e., on December 10, 2024. This act shall take effect on December 11, 2027. However, Chapter IV (Articles 35–51) shall apply from June 11, 2026, and Article 14 shall apply from September 11, 2026.

The entry into force of an EU regulation on the twentieth day after its publication is now standard practice. In assessing the rationality of such a standard time lag between publication and entry into force, the acceleration and facilitation of access to information on the law, linked to the electronic format of official journals and the development of legal search systems, is of significant importance.

The time gap between the entry into force and the application of an act draws attention, on the one hand, to the traditional identity of these terms in national law[39] and, on the other hand, to the fact that in Union law, an adjustment period begins on the date of entry into force. As emphasized in the literature, this is to enable legislators in EU Member States to supplement the provisions of the Regulation with the necessary national provisions implementing EU legislation. For public authorities and other entities, however, this period is intended to allow them to adapt to the requirements of the new provisions. In fact, it is sometimes shorter for entities obliged to apply the Regulation's provisions, as many issues are clarified in national provisions adopted later.[40] The CRA has accepted that its application will generally commence three years after it enters into

---

36 I. The general provisions (Articles 1–12); II. Obligations of economic operators and provisions on free and open-source software (Articles 13–26); III. Conformity of products with digital elements (Articles 27–34); IV. Notification of conformity assessment bodies (Articles 35–51); V. Market surveillance and enforcement (Articles 52–60); VI. Delegated powers and committee procedure (Articles 61–62); VII. Confidentiality and penalties (Articles 63–65); VIII. Transitional and final provisions (Articles 66–71).

37 Szpor, Gryszczyńska, and Wiewiórowski, eds., *Internet. Cyberodporność. Cyber Resilience*.

38 Sławomira Wronkowska, "O stanowieniu i ogłaszaniu prawa oraz o kulturze prawnej" [On the Enactment and Promulgation of Law and on Legal Culture], *Państwo i Prawo*, no. 4 (2007): 3–15.

39 Sławomira Wronkowska and Maciej Zieliński, *Komentarz do zasad techniki prawodawczej* [Commentary on the Principles of Legislative Technique] (Warsaw: Wolters Kluwer, 2004), 110.

40 Paweł Fajgielski, "Artykuł 99," in *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, 3rd ed., ed. Paweł Fajgielski (Warsaw: Wolters Kluwer, 2025), 794.

force. Therefore, the adjustment period seems long when compared, for example, to the General Data Protection Regulation, where it lasted two years. The assumption that it will be difficult and complicated is confirmed by the publications mentioned above.

The non-simultaneous commencement of the application of individual provisions of the new regulation is common in EU law. However, the need and possibility of early application of selected provisions may be questioned. It is, therefore, worth paying attention to the objectives, scope, and timetable for the early application of CRA provisions imposing obligations on public authorities and businesses.

A year and a half before the CRA comes into full effect, from June 11, 2026, Chapter IV, entitled "Notification of conformity assessment bodies," comprising as many as 17 articles (Articles 35–51), will apply. The rationale for this is already set out in Article 35, which stipulates that Member States shall notify the Commission and the other Member States of the bodies authorized to carry out conformity assessments in accordance with the CRA (paragraph 1) and shall endeavor to ensure that, by December 11, 2026 a sufficient number of notified bodies are designated in the Union to carry out conformity assessments, thereby avoiding bottlenecks and barriers to market entry (paragraph 2). To this end, each Member State shall designate a notifying authority (Article 36).

In addition, from September 11, 2026, the 10 comprehensive paragraphs of Article 14 CRA entitled "Reporting obligations of manufacturers" shall apply.[41] Paragraph 9 stipulates that, by December 11, 2025, the Commission shall adopt delegated acts in accordance with Article 61 of the CRA to supplement the CRA by specifying the conditions for applying cybersecurity considerations to the delay of the dissemination of notifications.[42] When preparing both draft delegated and implementing acts, the Commission is required to (as expressed in the operative part in paragraphs 9 and 10) cooperate with the CSIRT network established under Article 15 of Directive (EU) 2022/2555 and with ENISA, which will undoubtedly facilitate the clear establishment of a legal basis for this cooperation. During the adjustment period, the references in Chapter IV and Article 14 to provisions that will apply from December 2027 may raise doubts. However, it is worth noting that Article 61 of the CRA provides that the powers to adopt delegated acts, referred to, *inter alia*, in Article 14(9), shall be conferred on the Commission for a period of five years from December 10, 2024 (p. 2).[43] Before adopting a delegated act, the Commission shall consult experts designated by each Member State. A delegated act shall enter into force only if neither the European Parliament nor the Council has objected (p. 6).

The phased implementation of the provisions indicates that cyber resilience is understood as a process of building systemic capabilities, rather than a one-off state of compliance. The early start of the notification of conformity assessment bodies and

41 For a discussion of the CRA's model of vulnerability coordination and disclosure, see: Jukka Ruohonen and Paul Timmers, "Vulnerability Coordination under the Cyber Resilience Act," *Applied Cybersecurity & Internet Governance* 4, no. 1 (2025): 1–18, https://doi.org/10.48550/arXiv.2412.06261.

42 These are the notifications referred to in Article 16(2) of the CRA. Furthermore, as stated in paragraph 10, the Commission may, by means of implementing acts, specify the format and procedure for submitting the notifications referred to in Articles 14, 15, and 16.

43 The delegation of powers may be revoked at any time by the European Parliament or by the Council, by means of a decision, which shall not affect the validity of the delegated acts already in force.

the reporting obligations of manufacturers serves to create the institutional infrastructure necessary for the functioning of the market after 2027. The adjustment period is, therefore, a structural element of building systemic resilience, enabling the gradual internalization of new requirements by public authorities and businesses.

6. Conclusions

To meet the current challenges of digital transformation, in particular the development of the Internet of Things in the EU, horizontal cybersecurity requirements for products with digital elements have been established by a regulation of the European Parliament and of the Council.

The term "cyber resilience," contained in the short title of Regulation 2024/2847, has no legal definition, so its meaning needs to be established. It is used with rapidly increasing frequency in publications in various fields of science, but is explained in different ways. The relationship between cyber resilience and cybersecurity, and their place in the conceptual framework of digital transformation, remains unclear.

The legal and doctrinal analysis of the CRA, including its systemic interpretation, sets the framework for interpretation. The preamble confirms that the EU legislator refers to cyber resilience not only in relation to products with digital elements, but also in various other contexts. The manner in which the scope and exemptions in Article 2 are defined shows that the horizontal CRA is not a complete regulation for the cyber resilience of products with digital elements, but rather, a leading act that brings together the scattered standards relating to such products across many acts. The list of definitions shows that the cyber resilience of products subject to the regulation is built on a legally binding conceptual framework for digital transformation. On the other hand, this framework specifies the future in a broader scope than just products with digital elements. The extension of the time gap between entry into force and the start of full application highlights the new obligations of EU and national public authorities and businesses, the fulfillment of which is a necessary prerequisite for strengthening cyber resilience.

The CRA's analysis confirms the hypothesis that the concept of cyber resilience has untapped potential for increasing the consistency and transparency of the law, which is essential for its effectiveness. The result is a proposal to adopt a general definition of cyber resilience as a systemic category, a higher-order concept capable of integrating scattered sectoral regulations and performing an organizing function for digital transformation processes in legal doctrine. A starting point in this direction could be to adopt the definition that cyber resilience is the ability to cope with security challenges related to the digital transformation. As a legal concept, it refers to products with digital elements, as well as social and economic processes, information, and political-organizational systems. It includes detecting and reducing threats, responding to undesirable events and achieving objectives despite various disruptions: intentional and accidental, natural and man-made. Such a reconstruction also shows that cyber resilience is not limited to a single area of regulation, but has integrative potential.

An analysis of the abbreviated titles of EU regulations and directives, and their use in the practical interpretation and application of law in the area of digital transformation also leads to calls for a change in EU legislative principles, moving away from their adoption only in exceptional cases and, in addition, possibly indicating objectives and values in their content.

References

Björck, Fredrik, Martin Henkel, Janis Stirna, and Jelena Zdravkovic. "Cyber Resilience – Fundamentals for a Definition." In *New Contributions in Information Systems and Technologies*. Vol. 1, edited by Alvaro Rocha, Ana Maria Correia, Sandra Costanzo, and Luis Paulo Reis, 311–16. Cham: Springer, 2015. https://doi.org/10.1007/978-3-319-16486-1_31.

Chiara, Pier Giorgio. "Understanding the Regulatory Approach of the Cyber Resilience Act: Protection of Fundamental Rights in Disguise?." *European Journal of Risk Regulation* 16, no. 2 (2025): 469–84. https://doi.org/10.1017/err.2025.9.

Czerniawski, Michał. "Artykuł 93." In *Akt o usługach cyfrowych. Komentarz* [*Digital Services Act. Commentary*] edited by Dominik Lubasz and Monika Namysłowska. Warsaw: Wolters Kluwer, 2024. SIP LEX.

Dygnatowski, Sławomir. "Cyber Security as a Foundation for the Security of Critical Infrastructure in the Context of Modern Threats." *Journal of Konbin* 50, no. 4 (2020): 309–20. https://doi.org/10.2478/jok-2020-0089.

Fajgielski, Paweł. "Artykuł 99." In *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, 3rd ed., edited by Paweł Fajgielski, 794. Warsaw: Wolters Kluwer, 2025.

Hausken, Kjell. "Cyber Resilience in Firms, Organizations and Societies." *Internet of Things* 11 (2020): 100204. https://doi.org/10.1016/j.iot.2020.100204.

Jaroszyński, Tomasz. *Rozporządzenie Unii Europejskiej jako składnik systemu prawa obowiązującego w Polsce* [European Union Regulation as a Component of the Legal System in Force in Poland]. Warsaw 2011. LEX/el.

Linkov, Igor, and Alexander Kott. "Fundamental Concepts of Cyber Resilience: Introduction and Overview." In *Cyber Resilience of Systems and Networks: Risk, Systems and Decisions*, edited by Alexander Kott and Igor Linkov, 1–25. Cham: Springer, 2019. https://doi.org/10.1007/978-3-319-77492-3_1.

Pilarski, Grzegorz. "Tackling Cyberspace Threats: The International Approach." *Security and Defence Quarterly* 12, no. 3 (2016): 100–17. https://doi.org/10.35467/sdq/103238.

Ruohonen, Jukka, and Paul Timmers. "Vulnerability Coordination under the Cyber Resilience Act." *Applied Cybersecurity & Internet Governance* 4, no. 1 (2025): 1–18. https://doi.org/10.48550/arXiv.2412.06261.

Silicki, Krzysztof. "Cyberodporność wspierana przepisami prawa UE: akt o cyberodporności (CRA) i dyrektywa NIS 2" [Cyber Resilience Supported by EU Laws: Cyber Resilience Act and NIS2 Directive]. In *Internet. Cyberodporność. Cyber Resilience*, edited by Agnieszka Gryszczyńska, Grażyna Szpor, and Wojciech R. Wiewiórowski, 105–18. Warsaw: C.H. Beck, 2025.

Skoczylas, Dominika. "Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń" [Strengthening the European Union's Cybersecurity Capabilities: Cyber Solidarity in the Context of Cyber Threats]. *Europejski Przegląd Sądowy*, no. 12 (2024): 39–44.

Szafrański, Bolesław, ed. *Cyberbezpieczeństwo: redefinicja zagrożeń* [Cybersecurity: Redefining Threats]. Warsaw: Wojskowa Akademia Techniczna, 2023.

Szpor, Grażyna. "Introduction." In *Internet. Cyberodporność. Cyber Resilience*, edited by Agnieszka Gryszczyńska, Grażyna Szpor, and Wojciech R. Wiewiórowski, LXI. Warsaw: C.H. Beck, 2025.

Szpor, Grażyna. "Prawa jednostki i wspólnoty w Cyfrowej Dekadzie" [Rights of Individuals and Communities in the Digital Decade]. In *W trosce* o *dobro wspólnoty i jednostki – zagadnienia administracyjnoprawne*. *Księga jubileuszowa dedykowana Profesor Zofii Duniewskiej* [For the Good of the Community and the Individual – Administrative and Legal Issues. Jubilee Book Dedicated to Professor Zofia Duniewska], edited by Barbara Jaworska-Dębska, Monika Kapusta, Aneta Kaźmierska-Patrzyczna, Piotr Korzeniowski, Anna Król, Ewa Olejniczak-Szałowska, Agnieszka Rabiega-Przyłęcka, and Przemysław Wilczyński. Warsaw: Wolters Kluwer, 2024. LEX/el.

Szpor, Grażyna, and Paweł Hajduk. "Współdziałanie w egzekwowaniu przepisów z zakresu cyberbezpieczeństwa" [Cooperation in the Enforcement of Cybersecurity Regulations]. In *Cyberbezpieczeństwo. Współpraca versus konfrontacja informacyjna.* [Cybersecurity: Cooperation versus Informational Confrontation] ed. Bolesław Szafrański, 297–307. Warsaw: Wojskowa Akadema Techniczna, 2025.

van 't Schip, Mattis. "The Cyber Resilience Act and Open-Source Software: A Fine Balancing Act." *Journal of Intellectual Property, Information Technology and E-Commerce Law* 16, no. 1 (2025): 73–87.

Wiewiórowski, Wojciech R. "Europejskie rozumienie cyberodporności" [European Understanding of Cyber Resilience]. In *Internet. Cyberodporność. Cyber Resilience*, edited by Agnieszka Gryszczyńska, Grażyna Szpor, and Wojciech R. Wiewiórowski, 95–104. Warsaw: C.H. Beck, 2025.

Wikipedia. "Cyber Resilience." https://en.wikipedia.org/wiki/Cyber_resilience.

Wronkowska, Sławomira. "O stanowieniu i ogłaszaniu prawa oraz o kulturze prawnej" [On the Enactment and Promulgation of Law and on Legal Culture]. *Państwo i Prawo*, no. 4 (2007): 3–15.

Wronkowska, Sławomira, and Maciej Zieliński. *Komentarz do zasad techniki prawodawczej* [Commentary on the Principles of Legislative Technique]. Warsaw: Wolters Kluwer, 2004.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 117–132
https://doi.org/10.31743/recl.19283
Received: 27 November 2025 | Accepted: 17 December 2025 | Published: 31 March 2026

The EU AI Act and the Rights-Based Approach to Technological Governance

Georgios Pavlidis
Associate Professor of International and EU Law, Director of the Jean Monnet Center of Excellence AI-2-TRACE-CRIME, Neapolis University Pafos (NUP), School of Law; correspondence address: Neapolis University Pafos, Office 253, Danaes Avenue 2, Pafos 8042, Cyprus; e-mail: g.pavlidis@nup.ac.cy
https://orcid.org/0000-0001-6311-3086

Abstract: The European Union AI Act constitutes an important development in shaping the Union's digital regulatory architecture. The Act places fundamental rights at the heart of a risk-based governance framework. The article examines how the AI Act institutionalizes a human-centric approach to AI and how the AI Act's provisions explicitly and implicitly embed the protection of rights enshrined in the EU Charter of Fundamental Rights. It argues that fundamental rights function not merely as aspirational goals, but as legal thresholds and procedural triggers across the life cycle of an AI system. The analysis suggests that the AI Act has the potential to serve as a model for rights-preserving AI systems, while acknowledging that challenges will emerge at the level of implementation.

Keywords: Fundamental Rights, AI Act, EU Charter of Fundamental Rights, Risk-Based Approach, Human-Centric AI

1. Introduction

The Artificial Intelligence Act (AI Act)[1] of the European Union (EU) is the first comprehensive attempt by a major jurisdiction to regulate artificial intelligence (AI) through a horizontal legal framework, which follows a risk-based approach (RBA).[2] The AI Act was published in the Official Journal of the European Union on July 12, 2024, and entered into force on August 1, 2024. While its general application is scheduled for August 2, 2026, several provisions are subject to phased application, with certain obligations becoming applicable as early as 2025 and others deferred until 2027. The objective of the AI Act is to ensure the development and use of AI systems in alignment with the core values of the EU, including the protection of fundamental rights, as guaranteed by the Charter of Fundamental Rights of the European Union (the Charter).[3] Earlier EU initiatives, such

1 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (OJ L 2024/1689, 12 July 2024).

2 This approach has been used in several regulatory contexts, such as anti-money laundering; Gauri Sinha, "Risk-Based Approach: Is It the Answer to Effective Anti-Money Laundering Compliance?," in *Assets, Crimes and the State: Innovation in 21st Century Legal Responses*, eds. Katie Benson, Colin King, and Clive Walker (London: Routledge, 2020), 52–65; Georgios Pavlidis, "Asset Recovery in the European Union: Implementing a 'No Safe Haven' Strategy for Illicit Proceeds," *Journal of Money Laundering Control* 25, no. 1 (2022): 109, https://doi.org/10.1108/JMLC-11-2020-0131.

3 Charter of Fundamental Rights of the European Union (OJ C 326/391, 26 October 2012).

ISSN 2545-384X (Online)

as the General Data Protection Regulation (GDPR)[4] or the Digital Services Act (DSA),[5] address specific aspects of data protection or content moderation. However, unlike these initiatives, the AI Act integrates fundamental rights considerations across the entire life cycle of AI systems. The AI Act treats fundamental rights not as ancillary issues, but as part of legal obligations. This article examines how fundamental rights are integrated into the structure and logic of the AI Act. Special attention is given to the dynamic mechanisms, such as conformity assessments and institutional oversight, that are conditioned by the protection of fundamental rights. It is argued that the AI Act employs a model of rights-driven technological governance, using formal prohibitions, risk classifications, and continuous oversight grounded in the Charter.

2. The Rights-Based Approach: The Normative Compass of the AI Act

Article 1 of the AI Act sets the tone for the entire Regulation by aligning the development and deployment of AI systems[6] with the protection of fundamental rights, in compliance with the Charter of Fundamental Rights of the European Union. This reflects a strong commitment by the EU to ensure that the advancement of AI does not come at the expense of human dignity, privacy, non-discrimination, and other core rights.[7] Since the AI Act aims to promote "human-centric"[8] and "trustworthy"[9] AI, it acknowledges that technological innovation must serve people, not override their freedoms. Article 1 thus functions as both a declaratory provision and a normative compass, ensuring that innovation does not sideline fundamental rights, but instead reinforces them in the digital era. In practical terms, this means that all subsequent rules of the AI Act must be interpreted through the lens of fundamental rights.

The territorial, personal, and material scope of application of the AI Act reinforces the protection of fundamental rights by adopting an expansive approach. Indeed, Article 2(1)(c) ensures that the AI Act applies extraterritorially: even if AI providers[10]

4 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 119/1, 4 May 2016).

5 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)(OJ L 277/1, 27 October 2022).

6 According to Article 3(1) AI Act, "AI system" means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

7 Recitals 1 and 2 AI Act.

8 Joanna Bryson and Andreas Theodorou, "How Society Can Maintain Human-Centric Artificial Intelligence," in *Human-Centered Digitalization and Services*, eds. Marja Toivonen and Eveliina Saari (Singapore: Springer, 2019), 305–23.

9 Luciano Floridi, *Ethics, Governance, and Policies in Artificial Intelligence* (Cham: Springer, 2021), 41–5.

10 Under Article 3(3) AI Act, "provider" means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

or deployers[11] are established outside the EU, they fall within scope when their AI systems produce outputs that are used within the Union. This will help mitigate external threats, such as discriminatory or manipulative AI systems deployed transnationally.[12] Article 2(1)(g) makes it clear that the AI Act applies when people affected by an AI system are located within the EU. This puts individuals and their rights at the heart of the Regulation's scope, in line with the Charter's focus on personal dignity and protection. For its part, Article 2(4) adds an important nuance: it allows certain public authorities and international organizations to be exempt from the Act when they are working within the context of international cooperation in law enforcement or judicial matters. However, this exemption only applies if there are adequate safeguards in place to protect fundamental rights and freedoms, which is a recurrent concern in international police or judicial cooperation.[13] Such safeguards are important in cross-border contexts,[14] which can be prone to weaker oversight.

The AI Act defines key concepts that shape the interpretation and application of the rules on AI governance, including important references to fundamental rights. Two definitions stand out for their explicit rights-based dimension. First, the definition of a "serious incident" under Article 3, point (49) of the AI Act includes not only physical harm or disruption to infrastructure, but also incidents that result in "the infringement of obligations under Union law intended to protect fundamental rights."[15] Thus, breaches of rights, such as violations of privacy, non-discrimination, or due process, are treated with the same gravity as harms to human life and health, property, and infrastructure. This reflects an understanding that the harms caused by AI systems are not limited to physical consequences, but include insidious or systemic interferences with fundamental rights.[16] Second, the definition of "systemic risk" in Article 3, point (65), extends the notion of risk to include negative effects on fundamental rights and society as a whole, particularly from general-purpose AI models with high-impact capabilities. Therefore, these rights-sensitive concepts are integrated at the definitional level, affecting the interpretation of all subsequent provisions.

Another protective function of the AI Act is to categorically prohibit certain AI practices because they are deemed incompatible with the values and fundamental rights

11 Under Article 3(4) AI Act, "deployer" means a natural or legal person, public authority, agency, or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

12 Huw Roberts et al., "Global AI Governance: Barriers and Pathways Forward," *International Affairs* 100, no. 3 (2024): 1275, https://doi.org/10.1093/ia/iiae073.

13 Giulio Calcara, "Balancing International Police Cooperation: INTERPOL and the Undesirable Trade-off Between Rights of Individuals and Global Security," *Liverpool Law Review* 42, no. 2 (2021): 111, https://doi.org/10.1007/s10991-020-09266-9.

14 Recital 3 AI Act.

15 Recital 155 AI Act.

16 Francesca Palmiotto, "The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation," *European Journal of Risk Regulation* 16, no. 2 (2025): 770–93, https://doi.org/10.1017/err.2024.97.

under the EU Charter.[17] Among these practices, Article 5(1)(h) addresses a very controversial application of AI: "real-time" remote biometric identification systems[18] in publicly accessible spaces for law enforcement purposes. The default prohibition of such practices reflects serious concerns over their potential to undermine rights to privacy and data protection (Articles 7 and 8 of the Charter), freedom of assembly (Article 12), and non-discrimination (Article 21), as well as broader risks to democratic participation.[19] This preventive logic echoes the Court of Justice's reasoning in *Digital Rights Ireland*, where it held that large-scale, indiscriminate technological interferences with privacy and data protection are incompatible with the Charter, unless strictly necessary and proportionate, thereby reinforcing the rights-based limits on biometric surveillance.[20] The legislative text also introduces some narrowly tailored exceptions, which apply to exceptional circumstances, such as a targeted search for specific victims of abduction, trafficking in human beings, or sexual exploitation of human beings, the search for missing persons, as well as the prevention of imminent threats to life, or a "present, or genuine and foreseeable, threat of a terrorist attack," or the pursuit of serious criminal offences.[21] Even then, Article 5(2) requires a proportionality assessment that is context-sensitive. Furthermore, the use of such systems by law enforcement authorities is conditioned on a fundamental rights impact assessment (FRIA)[22] under Article 27 and prior registration in the EU database (Article 49).[23] These conditions promote accountability in the use of AI systems for "real-time" remote biometric identification. Real time biometric surveillance, even when exceptionally permitted, must be treated as a last resort, bounded by legal safeguards and the principle of necessity.[24] The objective is to protect the public sphere and curtail techno-authoritarian tools and indiscriminate biometric surveillance in a pre-emptive manner.[25]

3. The Rights-Based Approach in the Case of High-Risk AI Systems

In addition to the rules on prohibited AI systems, the AI Act introduces the classification of "high-risk" AI systems, triggering stringent obligations. Article 6, read in

17 Rostam J. Neuwirth, "Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA)," *Computer Law & Security Review* 48 (2023): 105798, https://doi.org/10.1016/j.clsr.2023.105798.

18 Article 3 (41) and (42) AI Act.

19 Recitals 32 ff AI Act.

20 CJEU Judgment of 8 April 2014, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

21 Annex II AI Act.

22 Recital 96 AI Act.

23 Recital 131 AI Act.

24 Arvind Jaiswal and Sandhya Tarar, "Real-Time Biometric System for Security and Surveillance Using Face Recognition," in *Advances in Computing and Data Sciences: 4th International Conference, ICACDS 2020, Valletta, Malta, April 24–25, 2020, Revised Selected Papers*, eds. Mayank Singh et al. (Singapore: Springer, 2020), 293–304, https://doi.org/10.1007/978-981-15-6634-9.

25 Hendrik Schopmans and İrem Tuncer Ebetürk, "Techno-Authoritarian Imaginaries and the Politics of Resistance Against Facial Recognition Technology in the US and European Union," *Democratization* 31, no. 5 (2024): 943–62, https://doi.org/10.1080/13510347.2023.2258803.

conjunction with Annex III, defines the criteria for such designations. Categories of "high-risk" AI systems include biometrics, critical infrastructure, education and vocational training, employment, workers' management and access to self-employment, access to and enjoyment of essential private services and essential public services and benefits, law enforcement, migration, asylum and border control management, administration of justice, and democratic processes.[26] An AI system listed in Annex III is presumed to be high-risk, unless it demonstrably does not pose a significant risk to health, safety, or fundamental rights. Therefore, the AI Act introduces a threshold for certain categories of systems that may threaten fundamental rights, although it could be argued that the standard of "significant risk to fundamental rights" leaves room for uncertainty and needs detailed interpretive guidance. Article 6(3) also introduces certain narrowly defined conditions under which an AI system may escape the high-risk classification, where it does not pose a significant risk of harm to the health, safety, or fundamental rights of natural persons, including by not materially influencing the outcome of decision-making. In this context, the AI system must be intended to perform a narrow procedural task or improve the result of a previously completed human activity; detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review; or perform a preparatory task for an assessment relevant for the purposes of the use cases listed in Annex III. The exemptions under Article 6 are carefully delimited, and they do not apply if the AI system performs profiling of natural persons.[27] Such profiling inherently raises serious fundamental rights concerns, including the rights to privacy, dignity, and equality.[28]

Another important compliance obligation concerns the establishment of risk management systems for high-risk AI systems.[29] Such systems, grounded in Article 9, must encompass risks to fundamental rights, alongside risks to health and safety.[30] This is another example of the AI Act's rights-based approach. Risks to fundamental rights, such as privacy, non-discrimination, due process, and freedom of expression, must be identified, analyzed, evaluated, and mitigated throughout the entire life cycle of the AI system. Providers are mandated to assess not only known risks, but also reasonably foreseeable risks to fundamental rights. This compels proactive engagement with how the AI systems might impact individuals and groups in the real world, including in ways not initially intended. Reasonably foreseeable misuses[31] must be avoided, because fundamental rights can be violated not only by flawed design, but also by predictable deployment patterns, such as biased training data. Moreover, there is a requirement to integrate insights

26 Ali Sunyaev et al., "High-Risk Artificial Intelligence," *Business & Information Systems Engineering* 67 (2025): 981, https://doi.org/10.1007/s12599-025-00942-6.

27 The term "profiling" is defined in Article 4, point (4) of GDPR.

28 Laurie N. Hobart, "AI, Bias, and National Security Profiling," *Berkeley Technology Law Journal* 40, no. 1 (2025): 165–231, https://doi.org/10.15779/Z38VX06474.

29 Jonas Schuett, "Risk Management in the Artificial Intelligence Act," *European Journal of Risk Regulation* 15, no. 2 (2024): 367–85, https://doi.org/10.1017/err.2023.1.

30 Recital 67 AI Act.

31 Article 3(13) AI Act.

from post-market monitoring systems,[32] which creates a feedback loop and enhances accountability.

In addition to risk management systems, the AI Act introduces another safeguard: the protection of fundamental rights through data governance.[33] Data is the foundation on which AI systems are trained and perform.[34] Therefore, flawed or biased data can translate into discriminatory outcomes, violations of privacy, and other systemic injustices.[35] High-risk AI systems must be developed using training, validation, and testing data sets that meet stringent criteria, precisely to prevent such harms. Among these criteria, Article 10(2)(f) explicitly requires examination of data sets for biases that are likely to affect health and safety, or have a negative impact on fundamental rights.

4. Procedural and Substantive Safeguards for the Protection of Fundamental Rights

4.1. Transparency Obligations and Fundamental Rights

The AI Act recognizes the significant role of transparency in protecting fundamental rights.[36] Article 13 specifically requires that the design of high-risk AI systems must enable deployers to understand and appropriately use the AI outputs. This is important, since deployers may not have the necessary technical expertise to identify and mitigate risks to privacy, non-discrimination, due process, or access to services. Transparency becomes a design feature of high-risk AI systems, rather than a fix that is applied *post hoc*.[37] This is a preventive approach that integrates the awareness of fundamental rights into the architecture of high-risk AI systems.[38]

The AI Act explicitly links transparency to the protection of fundamental rights, and it requires providers to disclose any foreseeable risks to health, safety, or fundamental rights resulting from both intended use and reasonably foreseeable misuse.[39] This is another anticipatory obligation, as used in other sections of the Act, which empowers deployers to assess the real-world, human impact of the AI system and adjust their practices

---

32 Jakob Mökander et al., "Conformity Assessments and Post-Market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation," *Minds and Machines* 32, no. 2 (2022): 241–68, https://doi.org/10.1007/s11023-021-09577-4.

33 Marijn Janssen et al., "Data Governance: Organizing Data for Trustworthy Artificial Intelligence," *Government Information Quarterly* 37, no. 3 (2020): 101493, https://doi.org/10.1016/j.giq.2020.101493.

34 Bogdan Fischer and Agnieszka Piskorz-Ryń, "Artificial Intelligence in the Context of Data Governance," *International Review of Law, Computers & Technology* 35, no. 3 (2021): 419–28, https://doi.org/10.1080/13600869.2021.1950925.

35 Recital 66 AI Act.

36 Nagadivya Balasubramaniam et al., "Transparency and Explainability of AI Systems: From Ethical Guidelines to Requirements," *Information and Software Technology* 159 (2023): 107197, https://doi.org/10.1016/j.infsof.2023.107197.

37 Heike Felzmann et al., "Towards Transparency by Design for Artificial Intelligence," *Science and Engineering Ethics* 26, no. 6 (2020): 3333, https://doi.org/10.1007/s11948-020-00276-4.

38 Ognyan Seizov and Alexander J. Wulf, "Artificial Intelligence and Transparency: A Blueprint for Improving the Regulation of AI Applications in the EU," *European Business Law Review* 31, no. 4 (2020): 611–40, https://doi.org/10.54648/eulr2020024; Recital 72 AI Act.

39 Article 13(3) point (b)(iii) AI Act.

accordingly.[40] There are additional requirements, such as providing information relevant to explainability, performance across demographic groups, and data specifications.[41] These requirements are tied to the right to non-discrimination and equal treatment, especially where the AI outputs may vary across populations. More broadly, transparency obligations under Article 13 serve as a safeguard for the right to good administration and the right to an effective remedy and to a fair trial (Articles 41 and 47 of the Charter).[42] Indeed, access to clear, comprehensible system documentation is a prerequisite for individuals to take legal action and contest adverse decisions based on AI outputs. In this respect, the emphasis on intelligibility and effective contestation aligns with the Court of Justice's approach in *Schrems II*, which stressed that formal legal safeguards are insufficient where individuals lack practical means to understand, challenge, or obtain redress against data-processing operations.[43] Meaningful transparency is important for affected persons, as it ensures that the logic behind decisions is not a "black box"[44] for the individuals whose rights are at stake.

4.2. Human Oversight as a Rights-Preserving Principle

Human oversight is another important safeguard in the governance of high-risk AI systems.[45] The AI Act introduces such oversight in its Article 14, as a mechanism to protect fundamental rights, alongside health and safety. The objective is that AI remains accountable to human judgment and does not operate in a normative vacuum.[46] This is particularly important where algorithmic outputs significantly affect people's lives, whether in policing, hiring, migration control, education, or access to welfare. Therefore, AI systems must be designed and developed in a way that allows oversight by natural persons. The AI Act affirms the principle that human agency must not be displaced by AI when decision-making can adversely affect individual rights and dignity. Oversight under Article 14(2) is essential for preventing or minimizing risks to fundamental rights, not just under intended use but also under reasonably foreseeable misuse. Oversight must be effective, not just symbolic. A similar concern was articulated by the European Court of Human Rights in *Big Brother Watch*, where the Court emphasized that human

40 Alessandro Mantelero, "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment," *Computer Law & Security Review* 34, no. 4 (2018): 754–72, https://doi.org/10.1016/j.clsr.2018.05.017.

41 Article 13(3) points (b)(iv) to (b)(vii) AI Act.

42 Kathleen Gutman, "The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?," *German Law Journal* 20, no. 6 (2019): 884–903, https://doi.org/10.1017/glj.2019.67; Izabela M. Wróbel, "Artificial Intelligence Systems and the Right to Good Administration," *Review of European and Comparative Law* 49, no. 2 (2022): 203–23, https://doi.org/10.31743/recl.13616.

43 CJEU Judgment of 16 July 2020, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559.

44 Georgios Pavlidis, "Unlocking the Black Box: Analysing the EU Artificial Intelligence Act's Framework for Explainability in AI," *Law, Innovation and Technology* 16, no. 1 (2024): 293–308, https://doi.org/10.1080/17579961.2024.2313795.

45 Riikka Koulu, "Proceduralizing Control and Discretion: Human Oversight in Artificial Intelligence Policy," *Maastricht Journal of European and Comparative Law* 27, no. 6 (2020): 720–35, https://doi.org/10.1177/1023263X20978649.

46 Recital 73 AI Act.

oversight mechanisms must be capable of providing real and continuous control over automated or large-scale surveillance systems, rather than operating as purely formal or *ex post* safeguards.[47] This concept anticipates deployment in real-world scenarios where discrimination and other violations of fundamental rights may arise unintentionally or through negligence. Of course, challenges remain regarding scalability, since oversight models may not scale effectively for high-volume, automated decisions. The AI Act gives some flexibility in how oversight is implemented. First, human oversight measures can be identified and built, when technically feasible, into the high-risk AI system (e.g., real-time alerts, override functions) by the provider before it is placed on the market or put into service. Second, such measures may be identified by the provider before placing the high-risk AI system on the market or putting it into service, which must be appropriate for implementation by the deployer. In both cases, the measures must be proportionate and context-sensitive. AI must not function as an unreviewable authority, and AI outputs must be contestable and corrigible by humans when fundamental rights are at stake. Thus, the AI Act gives practical effect to emerging principles, such as human-in-the-loop and human-on-the-loop,[48] taking into consideration the protection of fundamental rights, as discussed above.

4.3. Fundamental Rights Impact Assessment for High-Risk AI Systems

The AI Act introduces a significant procedural innovation: the mandatory Fundamental Rights Impact Assessment (FRIA) for certain deployers of high-risk AI systems.[49] An FRIA, as required under Article 27, deals with the use of AI in specific, sensitive contexts, such as public administration, law enforcement, and essential service provision, which can affect individuals' rights to privacy, non-discrimination, due process, education, and social protection. The AI Act requires public sector bodies and private entities performing public functions to assess such risks before the deployment of AI tools in these contexts. The nature of this accountability mechanism under Article 27 is clearly preventive.[50] The approach to the development of FRIAs is granular. Deployers must consider not only the system's technical characteristics, but also the context of its use in the real world. They are also required to consider the categories of individuals affected and the potential for harmful or discriminatory outcomes. This aligns with the Charter's focus on vulnerability, equality, and human dignity because deployers must assess specific risks to different groups, not just the general population. The AI Act further requires the FRIA to describe oversight mechanisms and redress arrangements, which is associated with

47 ECtHR Judgment of 25 May 2021, Big Brother Watch and Others v. United Kingdom, application nos. 58170/13, 62322/14 and 24960/15.

48 Therese Enarsson, Lena Enqvist, and Markus Naarttijärvi, "Approaching the Human in the Loop–Legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three Contexts," *Information & Communications Technology Law* 31 (2022): 123–53, https://doi.org/10.1080/13600834.2021.1958860.

49 Recital 96 AI Act.

50 Alessandro Mantelero, "The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template," *Computer Law & Security Review* 54 (2024): 106020, https://doi.org/10.1016/j.clsr.2024.106020.

the right to an effective remedy.[51] Deployers are allowed to rely on prior assessments, including assessments conducted by the provider, but such assessments must be kept up to date. The FRIA must also be notified to market surveillance authorities using a recordable and reviewable interface between AI deployment and public oversight. Finally, the FRIA complements, rather than duplicates, the Data Protection Impact Assessment (DPIA) required under the GDPR.[52] Thus, privacy and broader rights considerations are integrated into a unified compliance framework.[53] Nevertheless, it must be taken into account that FRIAs have limited applicability, in that they are binding only for specific categories of deployers, while practical guidance on their implementation remains under development. As a result, the FRIA functions not as a universal, *ex ante* obligation across all high-risk AI deployments, but as a targeted safeguard whose scope and operational content depend on both the classification of the system and the institutional role of the deploying actor.

4.4. Right to Explanation of Individual Decision-Making

The AI Act explicitly recognizes a right to explanation for individuals affected by decisions based on the output of high-risk AI systems.[54] This right, protected in Article 86, follows the logic of procedural fairness, transparency, and accountability. It operates as a prerequisite for the effective protection of fundamental rights, particularly in high-stakes contexts where algorithmic outputs influence access to services or opportunities in areas such as education, employment, credit, migration, and justice. At the same time, the right to explanation under the AI Act is conditional in scope and does not amount to a general or absolute entitlement applicable to all AI systems, but is instead linked to specific regulatory contexts, system classifications, and the nature of the decision-making process at issue. The right to explanation covers decisions taken by a deployer of a high-risk AI system (Annex III) that produce legal effects or similarly significant consequences. The right is triggered when the individual perceives the decision as having an adverse impact on their health, safety, or fundamental rights. This links the right to explanation to the implementation of the EU Charter, notably Articles 41 (right to good administration), 47 (right to an effective remedy), and 8 (protection of personal data). What makes Article 86 particularly impactful is that it requires not just a technical disclosure, but a "clear and meaningful explanation" of the following: (1) the role played by the AI system in the decision-making process, and (2) the main elements of the decision itself. The objective is to prevent "black-box" decisions that are unintelligible to the average

51 Angela Ward, "Remedies Under the EU Charter of Fundamental Rights," in *Research Handbook on EU Law and Human Rights*, eds. Sionaidh Douglas-Scott and Nicholas Hatzis (Cheltenham: Edward Elgar Publishing, 2017), 162–85.

52 Katerina Demetzou, "Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of 'High Risk' in the General Data Protection Regulation," *Computer Law & Security Review* 35, no. 6 (2019): 105342, https://doi.org/10.1016/j.clsr.2019.105342.

53 Article 27(4) AI Act.

54 Fleur Jongepier and Esther Keymolen, "Explanation and Agency: Exploring the Normative-Epistemic Landscape of the 'Right to Explanation'," *Ethics and Information Technology* 24, no. 49 (2022), https://doi.org/10.1007/s10676-022-09654-x.

person.[55] Such opaque decisions may impede access to redress or judicial review, undermining transparency and contestability, as discussed above. However, there are important limitations to the right to explanation, which does not apply where lawful exceptions are provided under Union or national law, and it only applies in the absence of similar rights already guaranteed elsewhere in EU law.[56] These exceptions are narrowly drawn and subject to Union law compliance. For this reason, they do not limit the importance of Article 86, which reflects the broader principles of human-centric, accountable, and contestable AI. In any case, it must be noted that, despite the right to explanation, the practical ability to challenge AI decisions remains rather constrained by information asymmetries and legal complexity.

5. Oversight and Enforcement through the Lens of Fundamental Rights

5.1. Tasks of the European Artificial Intelligence Board

The AI Act delineates the tasks of the European Artificial Intelligence Board (the Board), which functions as a coordinating and advisory body for the application of the AI Act across the Union. The protection of fundamental rights is a recurrent theme in the mandate of the Board.[57] This is most evident in several core responsibilities. First, the Board is tasked with facilitating coordination, harmonization of administrative practices, and the dissemination of best practices, including with respect to AI regulatory sandboxes, which themselves must mitigate fundamental rights risks, as discussed above. Moreover, the Board may issue recommendations and opinions on matters critical to fundamental rights governance, including revisions to Annex III (high-risk use cases) and Article 5 (prohibited practices), discussed above. The Board is also empowered to support AI literacy, public awareness, and understanding of safeguards and rights. The Board is also tasked with cooperating with EU agencies and networks in domains such as data and fundamental rights protection. Thus, the Board can function as a governance node that connects national authorities, the AI Office, the Commission, and broader civil society.[58] It is worth mentioning that the AI Act also establishes the Advisory Forum, a permanent, multistakeholder consultative body, to support the European AI Board and the Commission by offering technical expertise and strategic guidance.[59] The EU Agency for Fundamental Rights (FRA)[60] has been designated as a permanent member of the Advisory Forum, which guarantees a continuous and expert voice on fundamental rights

55 Margot E. Kaminski, "The Right to Explanation, Explained," in *Research Handbook on Information Law and Governance*, eds. Sharon Sandeen, Christoph Rademacher, and Ansgar Ohly (Cheltenham: Edward Elgar Publishing, 2021), 278–99.

56 For example, see Articles 15 or 22 GDPR.

57 Article 66 AI Act.

58 Claudio Novelli et al., "A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities," *European Journal of Risk Regulation* 16, no. 2 (2025): 566–90, https://doi.org/10.1017/err.2024.57.

59 Article 67 AI Act.

60 Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53/1, 22 February 2007).

in the discussions surrounding AI governance. The inclusion of ENISA[61] (cybersecurity) and the main European standardization bodies (CEN, CENELEC, and ETSI) further strengthens the role and expertise of the Forum at the intersection of rights, safety, and technical standards.

5.2. Designation of National Competent Authorities

At the level of enforcement, the AI Act requires each Member State to designate national competent authorities[62] and a single point of contact. Article 70(3) of the AI Act explicitly integrates fundamental rights protection into this institutional design; it requires that the designated authorities possess expertise not only in AI technologies, but also in personal data protection and fundamental rights. Therefore, the authorities tasked with monitoring and enforcing the AI Act cannot be merely technical regulators but must also be equipped to assess the legal and ethical implications of AI systems. Moreover, national competent authorities must act independently, impartially, and without bias, which aligns with the principles of institutional neutrality and accountability. This ensures the legitimacy of decisions taken by national authorities, especially when they deal with sensitive issues related to infringements of fundamental rights. Contact information for these authorities must be publicly available, enabling direct communication with affected persons, including for the lodging of complaints or access to redress mechanisms. Member States must also provide adequate resources and conduct regular assessments of authority competence and capacity to ensure that enforcement is operationally viable. Therefore, Member States must not merely transpose the AI Act formally, but actively build institutional ecosystems that can mitigate risks to fundamental rights across the AI life cycle. The key implementation challenge in this context relates to the diverging institutional capacities between Member States, which may lead to fragmented enforcement and uneven protection of fundamental rights.

5.3. Powers of Authorities Protecting Fundamental Rights

The AI Act establishes procedural mechanisms that empower national authorities tasked with enforcing fundamental rights, such as equality bodies, data protection authorities, or human rights institutions, to participate in the oversight of high-risk AI systems. Article 77 gives these authorities a legal basis to access all relevant documentation under the AI Act (risk assessments, technical specifications, post-market monitoring reports, and FRIAs). This must be provided in accessible language and format. The right of access to such documentation allows fundamental rights bodies to assess whether systems deployed in sensitive areas (Annex III) comply not only with the AI Act, but also with the Charter. Where documentation is insufficient, the authorities protecting fundamental rights can request

61 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151/15, 7 June 2019).

62 Emanuele Parisini and Eduard Dervishaj, "Emerging Models of National Competent Authorities Under the EU AI Act," *Annual International Conference on Digital Government Research* 26 (2025): 1, https://doi.org/10.59490/dgo.2025.1007.

technical testing of the AI system. This can uncover hidden biases or systemic effects that may not be apparent from documentation alone. Such testing must be carried out in close cooperation with the requesting authority. This is an example of a co-governance model, where both technical regulators and rights enforcers work together.[63]

5.4. Procedure at National Level for Dealing with AI Systems Presenting a Risk

The AI Act is integrated within the broader EU product safety regime.[64] The notion of a "product presenting a risk," under Article 79 of the AI Act, includes not only threats to health and safety, but also to fundamental rights. This constitutes an expansion of the traditional understanding of product risk. Market surveillance authorities can actively evaluate AI systems when they have reason to believe such systems present a risk, with particular attention to vulnerable groups. Indeed, the impacts of AI systems may be unevenly distributed, and certain groups, such as children, persons with disabilities, or migrants, may be disproportionately affected. When risks to fundamental rights are identified, the market surveillance authority must inform and cooperate fully with the relevant rights-protecting authorities. An enforcement leverage is ensured because the authorities have the power to require corrective actions, market withdrawal, or recall within short timelines.

5.5. AI Regulatory Sandboxes and Fundamental Rights

The AI Act establishes a framework for AI regulatory sandboxes, which are structured environments that enable the development and testing of innovative AI systems under regulatory supervision.[65] These sandboxes aim to promote innovation and market access, especially for SMEs and start-ups.[66] However, the protection of fundamental rights constitutes a condition of participation in these regulatory sandboxes, under Article 57 of the AI Act. This protective function is most evident in Article 57(6), which requires competent authorities supervising sandboxes to provide support not only on technical compliance, but also in identifying, assessing, and mitigating risks to fundamental rights. The inclusion of fundamental rights alongside health and safety throughout Article 57 confirms that innovation within the sandbox must respect specific boundaries. Article 57(11) further strengthens this precautionary approach by requiring authorities to suspend testing where significant rights risks cannot be effectively mitigated. Moreover, Article 57 integrates fundamental rights supervision into experimental AI development. Indeed, national data protection authorities and other relevant regulators must be associated with the operation and oversight of sandboxes where personal data or sectoral rights are involved. This ensures cross-disciplinary oversight. Thus, human rights expertise can be built into

63 Celso Cancela-Outeda, "The EU's AI Act: A Framework for Collaborative Governance," *Internet of Things* 27 (2024): 101291, https://doi.org/10.1016/j.iot.2024.101291.

64 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products (OJ L169/1, 25 June 2019).

65 Article 3(55) AI Act.

66 Thomas Buocz, Sebastian Pfotenhauer, and Iris Eisenberger, "Regulatory Sandboxes in the AI Act: Reconciling Innovation and Safety?," *Law, Innovation and Technology* 15, no. 2 (2023): 357–89, https://doi.org/10.1080/17579961.2023.2245678.

AI systems from the start, not added as an afterthought once the system is already in use. It must also be noted that participation in a regulatory sandbox does not entail blanket regulatory relief. While Article 57(12) of the AI Act allows for the mitigation of administrative fines where participants act in good faith and in compliance with the agreed sandbox plan and with the guidance of the competent authority, liability under EU and national law remains unaffected, thereby preserving victims' access to judicial and administrative redress. There is also emphasis on transparency and public accountability through exit reports, annual public reporting, and a dedicated interface for stakeholder engagement. All these measures comply with the broader, rights-based governance logic of the AI Act. Thus, regulatory sandboxes can become testbeds for responsible AI, ensuring that innovation remains aligned with fundamental rights. Of course, sandbox operations will depend significantly on the discretion of national authorities, which demonstrates the need for uniform, EU-wide standards in this context.

6. Conclusions

The AI Act seeks to answer how emerging technologies can be effectively regulated within liberal, democratic societies.[67] As demonstrated in this article, the protection of fundamental rights is integrated into several key provisions of the AI Act. The Charter is treated not merely as a guiding principle, but as a binding standard for AI governance. Several additional insights emerge from our analysis. First, fundamental rights serve as triggers for regulatory intervention (e.g., in determining high-risk systems), procedural obligations (e.g., transparency and human oversight), and enforcement actions (e.g., responses to compliant but harmful AI systems). Second, the AI Act introduces a dynamic model of governance, whereby the classification of AI systems, the obligations of providers and deployers, and the responsibilities of authorities can be calibrated to address new risks to fundamental rights. This constitutes a move away from static compliance models.

Although this article does not undertake a systematic, comparative analysis, the EU AI Act's rights-based regulatory architecture provides a meaningful reference point for transnational debates on AI governance. The EU model embeds fundamental rights as operative legal thresholds throughout the AI life cycle via risk classification, procedural safeguards, and institutional oversight. Thus, it contrasts with approaches that rely primarily on soft-law standards, sectoral guidance, or *ex post* accountability mechanisms. As such, the EU model offers a structured benchmark against which other emerging regulatory frameworks may be assessed, both within the Union and beyond, particularly in terms of how effectively they translate abstract rights commitments into enforceable procedural guarantees.

Of course, the effectiveness of the rights-based approach of the AI Act will depend on implementation. Translating the Act's provisions into meaningful safeguards requires not only technical expertise, but also institutional capacity, inter-agency cooperation, and civic engagement. Indeed, there are concerns about the operational readiness of national

[67] Andreas Jungherr, "Artificial Intelligence and Democracy: A Conceptual Framework," *Social Media + Society* 9, no. 3 (2023), https://doi.org/10.1177/20563051231186353.

authorities, the consistency of conformity assessments, and the meaningful participation of civil society and affected individuals. It is important that future amendments to the AI Act establish additional avenues for public input, redress, or meaningful contestation of high-risk system deployment. Moreover, tensions between innovation and regulation, between business competitiveness and rights protection, will continue to exist. Nonetheless, the AI Act sets an important precedent for how fundamental rights can be preserved in the digital age without retreating from technological change.

Funding: This study was funded by the European Union. Views and opinions expressed are, however, those of the author only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

References

Balasubramaniam, Nagadivya, Marjo Kauppinen, Antti Rannisto, Kari Hiekkanen, and Sari Kujala. "Transparency and Explainability of AI Systems: From Ethical Guidelines to Requirements." *Information and Software Technology* 159 (2023): 107197. https://doi.org/10.1016/j.infsof.2023.107197.

Bryson, Joanna, and Andreas Theodorou. "How Society Can Maintain Human-Centric Artificial Intelligence." In *Human-Centered Digitalization and Services*, edited by Marja Toivonen and Eveliina Saari, 305–23. Singapore: Springer, 2019.

Buocz, Thomas, Sebastian Pfotenhauer, and Iris Eisenberger. "Regulatory Sandboxes in the AI Act: Reconciling Innovation and Safety?." *Law, Innovation and Technology* 15, no. 2 (2023): 357–89. https://doi.org/10.1080/17579961.2023.2245678.

Calcara, Giulio. "Balancing International Police Cooperation: INTERPOL and the Undesirable Trade-off Between Rights of Individuals and Global Security." *Liverpool Law Review* 42, no. 2 (2021): 111–42. https://doi.org/10.1007/s10991-020-09266-9.

Cancela-Outeda, Celso. "The EU's AI Act: A Framework for Collaborative Governance." *Internet of Things* 27 (2024): 101291. https://doi.org/10.1016/j.iot.2024.101291.

Demetzou, Katerina. "Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of 'High Risk' in the General Data Protection Regulation." *Computer Law & Security Review* 35, no. 6 (2019): 105342. https://doi.org/10.1016/j.clsr.2019.105342.

Enarsson, Therese, Lena Enqvist, and Markus Naarttijärvi. "Approaching the Human in the Loop–Legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three Contexts." *Information & Communications Technology Law* 31 (2022): 123–53. https://doi.org/10.1080/13600834.2021.1958860.

Felzmann, Heike, Eduard Fosch-Villaronga, Christoph Lutz, and Aurelia Tamò-Larrieux. "Towards Transparency by Design for Artificial Intelligence." *Science and Engineering Ethics* 26, no. 6 (2020): 3333–61. https://doi.org/10.1007/s11948-020-00276-4.

Fischer, Bogdan, and Agnieszka Piskorz-Ryń. "Artificial Intelligence in the Context of Data Governance." *International Review of Law, Computers & Technology* 35, no. 3 (2021): 419–28. https://doi.org/10.1080/13600869.2021.1950925.

Floridi, Luciano. *Ethics, Governance, and Policies in Artificial Intelligence*. Cham: Springer, 2021.

Gutman, Kathleen. "The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?." *German Law Journal* 20, no. 6 (2019): 884–903. https://doi.org/10.1017/glj.2019.67.

Hobart, Laurie N. "AI, Bias, and National Security Profiling." *Berkeley Technology Law Journal* 40, no. 1 (2025): 165–231. https://doi.org/10.15779/Z38VX06474.

Jaiswal, Arvind, and Sandhya Tarar. "Real-Time Biometric System for Security and Surveillance Using Face Recognition." In *Advances in Computing and Data Sciences: 4th International Conference, ICACDS 2020, Valletta, Malta, April 24–25, 2020, Revised Selected Papers*, edited by Mayank Singh, Pankaj Gupta, Vikas Tyagi, Janusz Flusser, Tahar Ören, and Giuseppe Valentino, 293–304. Singapore: Springer, 2020. https://doi.org/10.1007/978-981-15-6634-9.

Janssen, Marijn, Paul Brous, Elsa Estevez, Luis S. Barbosa, and Tomasz Janowski. "Data Governance: Organizing Data for Trustworthy Artificial Intelligence." *Government Information Quarterly* 37, no. 3 (2020): 101493. https://doi.org/10.1016/j.giq.2020.101493.

Jongepier, Fleur, and Esther Keymolen. "Explanation and Agency: Exploring the Normative-Epistemic Landscape of the 'Right to Explanation'." *Ethics and Information Technology* 24, no. 49 (2022). https://doi.org/10.1007/s10676-022-09654-x/.

Jungherr, Andreas. "Artificial Intelligence and Democracy: A Conceptual Framework." *Social Media + Society* 9, no. 3 (2023). https://doi.org/10.1177/20563051231186353.

Kaminski, Margot E. "The Right to Explanation, Explained." In *Research Handbook on Information Law and Governance*, edited by Sharon Sandeen, Christoph Rademacher, and Ansgar Ohly, 278–99. Cheltenham: Edward Elgar Publishing, 2021.

Koulu, Riikka. "Proceduralizing Control and Discretion: Human Oversight in Artificial Intelligence Policy." *Maastricht Journal of European and Comparative Law* 27, no. 6 (2020): 720–35. https://doi.org/10.1177/1023263X20978649.

Mantelero, Alessandro. "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment." *Computer Law & Security Review* 34, no. 4 (2018): 754–72. https://doi.org/10.1016/j.clsr.2018.05.017.

Mantelero, Alessandro. "The Fundamental Rights Impact Assessment (Fria) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template." *Computer Law & Security Review* 54 (2024): 106020. https://doi.org/10.1016/j.clsr.2024.106020.

Mökander, Jakob, Maria Axente, Federico Casolari, and Luciano Floridi. "Conformity Assessments and Post-Market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation." *Minds and Machines* 32, no. 2 (2022): 241–68. https://doi.org/10.1007/s11023-021-09577-4.

Neuwirth, Rostam J. "Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA)." *Computer Law & Security Review* 48 (2023): 105798. https://doi.org/10.1016/j.clsr.2023.105798.

Novelli, Claudio, Philipp Hacker, Jessica Morley, Jarle Trondal, and Luciano Floridi. "A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities." *European Journal of Risk Regulation* 16, no. 2 (2025): 566–90. https://doi.org/10.1017/err.2024.57.

Palmiotto, Francesca. "The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation." *European Journal of Risk Regulation* 16, no. 2 (2025): 770–93. https://doi.org/10.1017/err.2024.97.

Parisini, Emanuele, and Eduard Dervishaj. "Emerging Models of National Competent Authorities Under the EU AI Act." *Annual International Conference on Digital Government Research* 26 (2025): 1–13. https://doi.org/10.59490/dgo.2025.1007.

Pavlidis, Georgios. "Asset Recovery in the European Union: Implementing a 'No Safe Haven' Strategy for Illicit Proceeds." *Journal of Money Laundering Control* 25, no. 1 (2022): 109–17. https://doi.org/10.1108/JMLC-11-2020-0131.

Pavlidis, Georgios. "Unlocking the Black Box: Analysing the EU Artificial Intelligence Act's Framework for Explainability in AI." *Law, Innovation and Technology* 16, no. 1 (2024): 293–308. https://doi.org/10.1080/17579961.2024.2313795.

Roberts, Huw, Emmie Hine, Mariarosaria Taddeo, and Luciano Floridi. "Global AI Governance: Barriers and Pathways Forward." *International Affairs* 100, no. 3 (2024): 1275–86. https://doi.org/10.1093/ia/iiae073.

Schopmans, Hendrik, and İrem Tuncer Ebetürk. "Techno-Authoritarian Imaginaries and the Politics of Resistance Against Facial Recognition Technology in the US and European Union." *Democratization* 31, no. 5 (2024): 943–62. https://doi.org/10.1080/13510347.2023.2258803.

Schuett, Jonas. "Risk Management in the Artificial Intelligence Act." *European Journal of Risk Regulation* 15, no. 2 (2024): 367–85. https://doi.org/10.1017/err.2023.1.

Seizov, Ognyan, and Alexander J. Wulf. "Artificial Intelligence and Transparency: A Blueprint for Improving the Regulation of AI Applications in the EU." *European Business Law Review* 31, no. 4 (2020): 611–40. https://doi.org/10.54648/eulr2020024.

Sinha, Gauri. "Risk-Based Approach: Is It the Answer to Effective Anti-Money Laundering Compliance?." In *Assets, Crimes and the State: Innovation in 21st Century Legal Responses*, edited by Katie Benson, Colin King, and Clive Walker, 48–62. London: Routledge, 2020.

Sunyaev, Ali, Alexander Benlian, Jella Pfeiffer, Ekaterina Jussupow, Scott Thiebes, Alexander Maedche, and Joshua Gawlitza. "High-Risk Artificial Intelligence." *Business & Information Systems Engineering* 67 (2025): 981–94. https://doi.org/10.1007/s12599-025-00942-6.

Ward, Angela. "Remedies Under the EU Charter of Fundamental Rights." In *Research Handbook on EU Law and Human Rights*, edited by Sionaidh Douglas-Scott and Nicholas Hatzis, 162–85. Cheltenham: Edward Elgar Publishing, 2017.

Wróbel, Izabela M. "Artificial Intelligence Systems and the Right to Good Administration." *Review of European and Comparative Law* 49, no. 2 (2022): 203–23. https://doi.org/10.31743/recl.13616.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 133–151
https://doi.org/10.31743/recl.19473
Received: 15 January 2026 | Accepted: 2 February 2026 | Published: 31 March 2026

Attributing Liability for Autonomous Vehicles: EU Multi-Level Approaches and Implications for Vietnamese Law

Dao Gia Phuc

PhD, Managing Director, Institute of International and Comparative Law, University of Economics and Law, Ho Chi Minh City, Vietnam and Vietnam National University, Ho Chi Minh City, Vietnam; correspondence address: 669 Do Muoi, Quarter 13, Linh Xuan Ward, Ho Chi Minh City, Vietnam; e-mail: phucdg@uel.edu.vn
https://orcid.org/0000-0003-0791-2152

Abstract: Autonomous vehicles (AVs) call into question the driver-centered premises of road traffic liability, as the task of driving becomes a distributed, socio-technical process involving software, sensors, updates, connectivity, infrastructure, and (sometimes) remote supervision. This article offers a doctrinal comparative analysis of how liability can be attributed across three axes, civil, administrative, and criminal, when accidents occur where there are higher levels of automation. It argues that the European Union does not (and need not) rely on a single AV liability code. Instead, EU law combines an insurance-first, victim-compensation logic with the modernization of product liability for software-enabled harms and a risk-based regulatory style that imposes documentation, post-market, and safety-management duties on upstream actors. Using Germany, France, and the Netherlands as illustrative models, the article maps Vietnamese law through the same framework. It shows that Vietnam already embodies a strong victim-protection baseline through strict "source of extraordinary danger" doctrines and is developing more stringent product responsibility tools. At the same time, Vietnam faces persistent mismatch risks in evidentiary access, cyber incident attribution, and the calibration of criminal accountability. The article concludes with a direction of reform, modified as appropriate for Vietnam, that preserves rapid compensation while structuring recourse, data governance, and controlled piloting.

Keywords: autonomous vehicles, liability allocation, compulsory motor insurance, product liability, Vietnam-EU comparative law

1. Introduction

While AVs are often discussed in terms of a technological leap forward, their most disruptive legal effect lies in how they reconfigure the basic grammar of road traffic responsibility. For over a century, accident law has treated driving as a human activity for which blame can be apportioned, insurance provided, and deterrents and prohibitions put in place. Higher levels of automation complicate this picture, since harm may be caused by a composite of machine perception, software inference, update management, connectivity, and organizational decisions about deployment, oversight, and operational design. The familiar binary system of "driver fault" versus "unavoidable accident" becomes less informative, while the social expectation of swift compensation remains unchanged. European legal debates are instructive not because the EU has produced a single model statute on AV liability, but because it has treated the problem as a multi-level design question. At the EU level, the baseline is primarily structured around two stable logics: (1) victim

ISSN 2545-384X (Online)

protection through compulsory motor insurance and loss-spreading, and (2) upstream accountability through product safety and product liability techniques that increasingly recognize software-enabled risks.[1] At the same time, Member States remain central to operational attribution as they define when the automated driving system is legally "in control," which human role (if any) is required to monitor, and what evidence architecture supports ex post reconstruction. The diversity of national solutions is not merely a fragmentation problem; it serves as a policy laboratory that reveals different ways to align compensation, deterrence, innovation, and legal certainty.

Vietnam enters this debate from a different starting point. It is often assumed that jurisdictions without large-scale, commercial AV deployment must first catch up in legislative terms. Vietnamese private law already embodies strong risk-allocation intuition through strict liability for hazardous sources, and Vietnam's recent consumer protection reforms strengthen product responsibility tools directly relevant to AV-caused harm.[2] These features position Vietnam not only as a policy-taker, but also as a practical comparative reference point, where Vietnam's doctrinal commitment to swift victim compensation highlights an enduring normative anchor that many European discussions share, even when the doctrinal pathways differ. At the same time, Vietnam faces distinctive "mismatch risks" if AVs arrive under current frameworks. Vietnam can draw several lessons from the EU's multi-level approach to AV liability. The European experience demonstrates the value of combining rapid victim compensation with clear avenues of upstream accountability. By observing how EU jurisdictions integrate compulsory insurance with product liability and targeted safety regulations, Vietnam can anticipate potential gaps and overlaps in its own regime. For example, Europe's diversity of national solutions offers Vietnam concrete models for balancing innovation and safety, showing that it is possible to encourage AV development (through controlled pilot programs and regulatory sandboxes) while still maintaining strong protection for accident victims. Vietnam can leverage these insights to craft a legal framework that avoids known pitfalls (such as evidentiary barriers or unclear responsibility gaps) and aligns with international best practices, rather than reinventing the wheel.

Methodologically, this article adopts a doctrinal, comparative approach, examining primary legal sources (statutes, directives, regulations, and case law) and scholarly commentary across jurisdictions. It relies on the EU's legal instruments (such as the Product Liability Directive and Motor Insurance Directive) and the illustrative national laws of Germany, France, and the Netherlands, juxtaposing them with Vietnamese civil, administrative, and criminal liability rules. Comparative analysis identifies functional equivalents and divergences, highlighting areas where Vietnam's legal framework converges with or departs from European approaches.

---

1 Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability; Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products (repealing Council Directive 85/374/EEC).

2 For Vietnam's developing smart vehicle governance baseline and the relevance of product responsibility reforms, see reporting on the Law on Road Traffic Safety and Order (in force: January 1, 2025) and the classification of smart vehicles into five levels.

2. Autonomous Vehicles Levels and Liability Architecture

2.1. Definition of AVs and Automation Levels

An autonomous vehicle (AV) is a vehicle equipped with an Automated Driving System (ADS), capable of controlling driving with minimal or no human intervention. The Society of Automotive Engineers (SAE) has defined six levels of driving automation, from Level 0 (no automation) up to Level 5 (full automation).[3] Only vehicles at SAE Level 3 and above are considered "self-driving" or autonomous, since at Level 3, the system can perform the task of driving under certain conditions, and higher levels entail even greater autonomy and less human control.[4] At Level 3 (Conditional Automation), the human driver is still expected to serve as a fallback and take over when the ADS so requests or when obvious system limits are reached. By Level 4 (High Automation), the vehicle can operate on its own within its defined operational design domain (ODD), without expecting a human to intervene, effectively making the human a passive occupant (sometimes termed a "technical supervisor" rather than a driver). Finally, Level 5 (Full Automation) envisions a vehicle capable of self-driving under all road and environmental conditions, with no human driving role at all.

2.2. Liability Architecture for Autonomous Vehicles

2.2.1. Civil Liability

When an autonomous or highly automated vehicle causes harm, civil liability remains the primary channel for victim compensation and the subsequent allocation of accident-related costs among the relevant actors.

Tort-based liability. Traditionally, traffic accidents have been governed by tort law principles of fault or negligence. However, many legal systems modify or replace fault-based rules with strict liability for motor vehicles, given that vehicles are inherently hazardous instrumentalities.[5] The policy behind such strict liability schemes is to distribute the risks connected with using advanced but dangerous technology among those who operate or benefit from it, and to compensate victims swiftly. On the other hand, if a human operator of an AV can be shown to have been negligent (for instance, by misusing the technology or failing to take over control when required at Level 3), traditional fault-based liability may still apply. In practice, jurisdictions are grappling with how these principles should be modified as human control diminishes.[6]

Product liability. Most jurisdictions have established product liability regimes that hold manufacturers strictly liable for harm caused by defective products, without requiring the victim to prove negligence.[7] This means that if an ADS or any component

---

3 Debbie Hopkins and Tim Schwanen, "Talking about Automated Vehicles: What Do Levels of Automation Do?," *Technology in Society* 64 (2021): 101488, https://doi.org/10.1016/j.techsoc.2020.101488.

4 Michael A. Gerber, Ronald Schroeter, and Bonnie Ho, "A Human Factors Perspective on How to Keep SAE Level 3 Conditional Automated Driving Safe," *Transportation Research Interdisciplinary Perspectives* 22 (2023): 100959, https://doi.org/10.1016/j.trip.2023.100959.

5 Ibid.

6 Hopkins and Schwanen, "Talking about Automated Vehicles."

7 Sara Vanetta, Christian M. Theissen, and Isabelle Peltier, "Navigating Product Liability in High-Security Sectors: Addressing AI-Driven Risks under German and European Law," White & Case LLP, December 16, 2025,

of an AV malfunctions in a way that causes an accident, the injured party can seek compensation from the producer under product liability law.[8] In the context of AVs, product liability is crucial because the "driver" may argue that the accident was caused by an autonomous decision or technical failure beyond their control. Indeed, as vehicles become more automated, the locus of responsibility shifts increasingly toward the entities that design and sell the technology. One practical challenge, however, is that determining whether an AV's performance was "defective" (i.e., did not meet reasonable safety expectations) can be complex. It may require technical reconstruction of what the vehicle saw or decided at the moment the defect occurred, often a difficult task when software algorithms are involved.

2.2.2. Administrative and Regulatory Compliance

Operators, owners, and manufacturers of AVs may be subject to specific compliance obligations, for example, keeping the vehicle's software up to date, performing required maintenance and safety checks, restricting the use of the AV to its approved ODD (i.e., a vehicle only certified for highway driving is not operated on urban streets or in adverse weather), and having a system in place for oversight when the vehicle is in autonomous mode. Failure to comply with these requirements can result in administrative sanctions, including fines, permit revocation, or other penalties.[9] If the supervisor or owner does not comply with these legal obligations, and thus ignores a mandatory safety update issued by the manufacturer or allows the vehicle to operate outside its legal parameters), they could face regulatory consequences. Thus, administrative law tools work in tandem with liability rules.

2.2.3. Criminal Liability

Criminal liability for road incidents (e.g., dangerous driving, vehicular manslaughter) traditionally presupposes a human driver who engages in blameworthy conduct (recklessness, gross negligence, etc.). However, when a vehicle is driving itself, the human occupant may be essentially a passenger, not actively controlling the motion.[10] In other words, if the autonomous system's actions (rather than a human's direct input) lead to a traffic violation, or even a collision, the human in the driver's seat would generally not be prosecuted for that outcome. Instead, responsibility shifts to the vehicle's makers and people maintaining it, as the incident would be handled as a regulatory matter by the Automated Driving System Entity (ADSE). This is typically the manufacturer or software provider, who would be investigated or sanctioned by regulators. In cases of egregious malfunction or safety lapses, this could even lead to corporate criminal liability, for instance,

accessed February 23, 2026, https://www.whitecase.com/insight-alert/navigating-product-liability-high-security-sectors-addressing-ai-driven-risks-under.

8 Tiago Sérgio Cabral, "Liability and Artificial Intelligence in the EU: Assessing the Adequacy of the Current Product Liability Directive," *Maastricht Journal of European and Comparative Law* 27, no. 5 (2020): 615–35, https://doi.org/10.1177/1023263X20948689.

9 Antonios E. Kouroutakis, "Autonomous Vehicles: Regulatory Challenges and the Response from Germany and UK," *Mitchell Hamline Law Review* 46, no. 5 (2020): 1103, https://open.mitchellhamline.edu/mhlr/vol46/iss5/3.

10 Chris Tennant et al., "Public Anticipations of Self-Driving Vehicles in the UK and US," *Mobilities* 20, no. 2 (2025): 292–309, https://doi.org/10.1080/17450101.2024.2325386.

prosecution under product safety laws or general criminal negligence if the company was reckless in deploying unsafe technology.

On the other hand, individuals may still face criminal charges, even if their own misconduct contributed to an AV incident. If a "driver" intentionally misuses the automation, for example, by engaging the self-driving mode in inappropriate conditions or ignoring a takeover request, traditional offenses like negligent homicide or endangerment could apply to that individual. Similarly, if an operator is required to be available (as in Level 3), but is found to be wilfully inattentive,[11] prosecutors may treat that as criminally negligent behavior on the part of the human.

3. EU Legal Framework for Autonomous Vehicle Liability and Member State Approaches

3.1. EU Level

3.1.1. Civil Liability

At the European Union level, there is currently no dedicated AV liability statute; instead, existing EU civil liability frameworks apply. The cornerstone is the Product Liability Directive (85/374/EEC), which imposes strict liability on manufacturers for defective products that cause damage.[12] Additionally, all EU Member States must implement the Motor Insurance Directive (2009/103/EC), which requires compulsory vehicle liability insurance, so that traffic victims are compensated regardless of fault.[13] Despite these frameworks, the EU currently lacks harmonized rules that explicitly divide liability between human users and automated systems.[14] Questions such as whether a human "driver" should be legally considered at fault when an automated driving feature is engaged are not yet uniformly answered at the EU level. In 2017, the European Parliament called for EU civil law rules on robotics (including AVs) to ensure consistency.[15] In response, the European Commission proposed an "AI Liability Directive" in 2022, as an aid in pursuit of victims' claims involving AI systems. However, it does not introduce new, substantive liability rules specific to AVs.[16] In parallel, the EU has been developing the AI Act, a regulatory regime that classifies AI systems by risk. Automated driving systems are considered "high-risk" AI,

11 Gerber, Schroeter, and Ho, "A Human Factors Perspective on How to Keep SAE Level 3 Conditional Automated Driving Safe," 3.

12 Ibid.

13 Eric Tjong Tjin Tai, "Civil Liability for Self-Driving Cars in Dutch Law," in *Autonomous Vehicles and Civil Liability in a Global Perspective*, eds. Hans Steege et al. (Cham: Springer, 2024), 385–403.

14 Didem Polad, "Liability Perspective for Users of Autonomous Vehicles in the EU," RAILS – Blog, April 15, 2024, accessed February 23, 2026, https://blog.ai-laws.org/liability-perspective-for-users-of-autonomous-vehicles-in-the-eu/.

15 Tatjana Evas, "A Common EU Approach to Liability Rules and Insurance for Connected and Autonomous Vehicles: European Added Value Assessment: Accompanying the European Parliament's Legislative Own Initiative Report," European Parliamentary Research Service, February 2018, accessed February 23, 2026, https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2018)615635.

16 Polad, "Liability Perspective for Users of Autonomous Vehicles in the EU."

so manufacturers will have to meet strict safety and compliance requirements under this forthcoming regulation.[17]

3.1.2. Administrative and Regulatory Framework

The EU has been proactive in establishing an administrative framework to integrate AVs safely. Notably, the EU General Safety Regulation (2019/2144) introduced a roadmap of new mandatory safety features from 2022 onwards, with event data recorders (EDR).[18] This evidentiary mechanism, mandated at the EU level, supports both civil and criminal proceedings by providing reliable data on vehicle behavior. Also, in August 2022, the EU implemented specific rules for ADS type-approval with Regulation (EU) 2022/1426. Soon after, Regulation (EU) 2022/2236 was adopted to allow small-series production of AVs without human controls, introducing adapted technical standards for completely driverless vehicles.[19] These regulations mark a significant step, as, for the first time, EU law permits vehicles with Level 4/5 automation (no driver onboard or no driver's seat at all) to be legally homologated (approved) for EU roads, provided they meet stringent safety benchmarks.

3.1.3. Criminal Liability Considerations

Unlike civil and regulatory matters, the EU has no unified criminal code for traffic incidents. However, EU-level efforts to implement the aforementioned data recorder mandates and technical requirements support criminal justice by ensuring that evidence is available and that vehicles are traceable in the event of offenses. This implies that Member States should update their own laws to assign responsibility (e.g., to the vehicle owner, operator, or manufacturer) for compliance with traffic laws when a vehicle is driving itself.

3.2. Member State Approaches

Given the absence of a single EU liability regime for autonomous vehicles, Member States have begun developing their own laws and models. Here are three illustrative approaches, those of Germany, France, and the Netherlands, across the three liability dimensions (civil, administrative, criminal).

3.2.1. Civil Liability

Germany. Under the German Road Traffic Act (Straßenverkehrsgesetz), the vehicle owner (keeper) is strictly liable for any damage to persons or property caused by the vehicle, and the driver faces fault-based liability for road accidents.[20] In 2017, Germany amended this law to address Level 3 automation, and in 2021, it passed an Autonomous Driving Act

17 Charles Kerrigan, Sean Musch, and Michael Borrelli, "The EU AI Act," in *Artificial Intelligence*, ed. Charles Kerrigan (Cheltenham: Edward Elgar Publishing, 2025), 178–239, https://doi.org/10.4337/9781035334353.00020.

18 Maria Cristina Galassi et al., "Safety Approval of Automated Vehicles in the EU: Moving Beyond Highway Applications," *Transportation Research Procedia* 72 (2023): 4396–403, https://doi.org/10.1016/j.trpro.2023.11.328.

19 For instance, requirements for failsafe mechanisms, cybersecurity, and software updates. See: Marcin Dziadkiewicz, "Technological Innovations in Transportation: Law and Practice," in *The Use of Information and Communication Technologies (ICT) in the Management of the Innovative and Smart City*, eds. Judyta Kabus, Luiza Piersiala, and Michał Dziadkiewicz (Boca Raton: CRC Press, 2024), 64–99.

20 Maurice Schellekens, "Self-Driving Cars and the Chilling Effect of Liability Law," *Computer Law & Security Review* 31, no. 4 (2015): 506–17, https://doi.org/10.1016/j.clsr.2015.05.012.

for Level 4 vehicles.[21] German law now distinguishes between the roles of a "Level 3 driver" and a "Level 4 technical supervisor." A Level 3 AV (where the human may cede driving tasks, but must resume control upon request) is still legally considered a human-driven vehicle. In contrast, at Level 4, fully autonomous driving, driving is overseen by a technical supervisor rather than a traditional driver. The technical supervisor is typically a person or entity that remotely monitors the vehicle. Under German law, the supervisor is liable under general tort principles (fault-based) instead of the strict/presumed fault regime.[22] If an accident occurs while the vehicle is under automated control (and not due to any supervisor intervention), liability may shift to the vehicle's manufacturer under product liability or system defect theories.[23] Thus, when the technology is truly at the helm (Level 4), the traditional driver-centric liability diminishes, and the manufacturer or system provider bears responsibility if a flaw in the automated system caused the harm.

France. France has a long-standing tradition of protecting road accident victims through strict driver liability, notably through the *Loi Badinter* of 1985.[24] Under the *Badinter* regime, any motor vehicle driver (or keeper) is almost automatically liable and required to compensate victims, such as pedestrians, cyclists, or passengers, except in limited circumstances (e.g., if an unforeseeable external event caused the accident). As AV technology advances, France faces the question of how to adapt this strict liability model. France's Mobility Orientation Law (Loi n° 2019–1428 – MOL) empowered the government to legislate for AV operations, and an Ordinance of 14 April 2021 (effective 2022) set out specific liability rules for automated vehicles.[25] Under this Ordinance (now codified in the Transport Code), when a vehicle is operating in an approved autonomous driving mode, the human "driver" is not civilly liable for accidents caused by the driving system.[26] Instead, responsibility for harm shifts to the vehicle manufacturer or the entity that deployed the automated system. If the human was supposed to take over but failed to do so, and thus ignored an explicit takeover request, the human could still be found to be at fault.[27]

Netherlands. Under Dutch law, the owner or keeper of a motor vehicle is strictly liable for any accident damage caused by that vehicle (Article 185 of the *Wegenverkeerswet* – Road Traffic Act).[28] This strict liability applies even if the vehicle was self-driving at the time of

21 Polad, "Liability Perspective for Users of Autonomous Vehicles in the EU."

22 Thus, this creates a different burden of proof: for Level 3 accidents, the human driver must prove they did nothing wrong to escape liability, whereas for Level 4 accidents, the injured party must prove the technical supervisor failed to meet their duty of care.

23 Benjamin von Bodungen and Hans Steege, "Liability for Automated and Autonomous Driving in Germany," in *Autonomous Vehicles and Civil Liability in a Global Perspective: Liability Law Study across the World in Relation to SAE J3016 Standard for Driving Automation*, eds. Hans Steege et al. (Cham: Springer, 2024), 279–320.

24 Polad, "Liability Perspective for Users of Autonomous Vehicles in the EU."

25 STRMTG, "The French Regulatory Framework for Automated Road Transport Systems (ARTS) Has Been Published," October 4, 2022, accessed February 23, 2026, https://www.strmtg.developpement-durable.gouv.fr/en/the-french-regulatory-framework-for-automated-road-a167.html.

26 Phillip Morgan, "Chapter 1: Tort Liability and Autonomous Systems Accidents – Challenges and Future Developments," in *Tort Liability and Autonomous Systems Accidents: Common Law and Civil Law Perspectives*, ed. Phillip Morgan (Northampton, MA: Edward Elgar Publishing, 2023), 1–26.

27 Polad, "Liability Perspective for Users of Autonomous Vehicles in the EU."

28 Tjong Tjin Tai, "Civil Liability for Self-Driving Cars in Dutch Law."

the accident. Thus, when a self-driving car in the Netherlands is involved in a crash, the victim will claim against the vehicle owner's motor insurer, who will pay out the damages. The insurer (or owner) can then seek recourse against the vehicle's manufacturer if a defect in the AV contributed to the accident.[29] Under Dutch law, the human driver can also be held liable if their negligence contributed to the accident.[30] A key question for higher automation is whether a human in a Level 4 or 5 vehicle is even expected to monitor the driving. Dutch legal scholars anticipate that courts may excuse the human from paying continuous attention in Level 4/5 scenarios, given that the technology is supposed to handle all driving tasks.[31] The Netherlands has not enacted a special AV liability law; instead, it relies on the flexible application of existing rules. The strict liability of vehicle owners provides a blanket of protection for victims (much like the French *Badinter* law), and the law already permits fault to be apportioned to manufacturers for product defects.

3.2.2. Administrative Liability

Germany. In 2017, Germany amended its traffic laws to legalize SAE Level 3 automated driving features, provided that a human driver remains seated and ready to intervene.[32] Building on that, the Act on Autonomous Driving (2021) enabled SAE Level 4 vehicles to operate regularly on public roads if they meet technical requirements, and if a technical supervisor is monitoring it (the supervisor can be remote).[33] The Federal Motor Transport Authority oversees a permit process under which the vehicles must obtain special approval to operate in automated mode in designated zones, and the operating entity must have safety protocols in place.[34] Thus, rather than using *ad hoc* exemptions, Germany codified a framework that allows manufacturers to seek type approval for Level 4 systems (aligned with EU standards), and for operators to deploy them with government authorization. Companies operating AVs must also appoint licensed supervisors who have completed specific training and can take over or shut down the vehicle if needed.[35] In terms of data and reporting, German law (§63a Road Traffic Act) mandates that AVs log operational data and make it available to authorities in the event of incidents.

France. In 2016, France began by allowing limited experimentation with self-driving cars on public roads (with safety drivers and permits). Later, the MOL of 2019 granted the government the authority to issue regulations governing AV deployment. France used this to establish a comprehensive regime in 2021. The Ordinance of 14 April 2021 (and the implementing Decree of 29 June 2021) set out the conditions under which AVs up to Level 4

29 Ibid.

30 For example, if a Level 2 or 3 car gave a handover warning that the human ignored, that human may be found negligent. See ibid.

31 Lena Wrzesniowska, "Can AI Make a Case? AI Vs. Lawyer in the Dutch Legal Context," *International Journal of Law, Ethics & Technology* 4, no. 3 (2024): 1.

32 Kouroutakis, "Autonomous Vehicles: Regulatory Challenges and the Response from Germany and UK."

33 Polad, "Liability Perspective for Users of Autonomous Vehicles in the EU."

34 For example, the law and its regulations specify that Level 4 AVs must have redundant systems, a remote monitoring control center, and fail-safe mechanisms to achieve a "minimal risk condition" (e.g., safe stop) if problems arise. See: Galassi et al., "Safety Approval of Automated Vehicles in the EU."

35 Polad, "Liability Perspective for Users of Autonomous Vehicles in the EU."

can be put into general operation on French roads.[36] Level 4 vehicles are permitted to operate without a driver on board but must be supervised by a remote operator and confined to predefined routes or areas.[37] Administratively, France assigns responsibilities to different actors, since the remote operator must have completed specific training and be capable of taking over or commanding the vehicle remotely: the AV system provider (manufacturer) must supply data access to regulators (to verify compliance and investigate incidents); and the service operator (if different from manufacturer) must implement security measures and ensure that vehicles meet technical requirements. France also created a scheme that holds automated vehicle providers liable for traffic fines and infractions.[38] This administrative rule, unique to France so far, incentivizes manufacturers to design obey-the-law behavior, as they will literally pay the price for traffic violations by their AI.

Netherlands. Rather than immediately overhauling laws, the Netherlands introduced the *Experimenteerwet* (Experimentation Law) for Self-Driving Vehicles, which came into force around 2018.[39] Under the experimental framework, companies or research institutions can apply for a permit from the Dutch Vehicle Authority (RDW) to test AVs on public roads without a human driver inside, as long as a human can supervise and control remotely.[40] This "learning by doing" approach allowed the Netherlands to host early pilots (e.g., automated shuttles, truck platooning) and gather data for assessment regarding permanent regulation.[41] As of the mid-2020s, the Netherlands has been working on transitioning from experimental mode to routine deployment. The Dutch will probably introduce an "Authorized Self-Driving System" operator model,[42] in which a company that operates an AV service is officially designated and accountable for that vehicle's compliance (effectively taking on the role of the driver in the eyes of the law). Administratively, the Netherlands currently employs a sandbox approach, administratively using permits and exemptions to allow AV operation, and is poised to formalize those practices into law once the technology matures.

---

36 STRMTG, "The French Regulatory Framework for Automated Road Transport Systems (ARTS) Has Been Published."

37 Jonas Knetsch, "La voiture autonome face au droit: les réponses en droit positif et en droit prospectif (Regards d'aujourd'hui vers le futur ?): Rapport français," in *Autonomous Vehicles and the Law*, ed. Gilles Pillet (Leiden: Brill–Nijhoff, 2025), 158–87, https://doi.org/10.1163/9789004711891_006.

38 Knetsch, "La voiture autonome face au droit."

39 This law created a mechanism for the government to exempt specific road traffic rules on a case-by-case basis to permit trials of driverless vehicles. To get approval, applicants must demonstrate robust safety measures, such as remote monitoring capabilities, fail-safe responses, and sufficient insurance coverage. The RDW, in coordination with road authorities and traffic safety experts, evaluates each test proposal individually, considering factors like location, time, traffic conditions, and whether a backup driver might trail or oversee the test. See: Ministerie van Infrastructuur en Waterstaat, "Mobility, Public Transport and Road Safety: Self-Driving Vehicles," 2025, accessed February 23, 2026, https://www.government.nl/topics/mobility-public-transport-and-road-safety/self-driving-vehicles.

40 Ibid.

41 K.A.P.C. van Wees, "Civil Liability for Autonomous Vehicles in the Netherlands," in *Autonomous Vehicles and the Law: A Revolution through the Prism of Civil Liability*, ed. Gilles Pillet (Leiden: Brill, 2025), 289–330, https://doi.org/10.1163/9789004711891_009.

42 Tjong Tjin Tai, "Civil Liability for Self-Driving Cars in Dutch Law."

3.2.3. Criminal Liability

Germany. In German law, traffic offenses and crimes (like dangerous driving or negligent homicide in a traffic accident) are predicated on a human actor's culpability.[43] With Level 3 automation, the human driver is still legally required to monitor the driving environment and to retake control when prompted or when obvious danger arises. Germany's 2017 amendment (Act on Automated Driving) implicitly acknowledged this by prohibiting drivers from fully relinquishing attention, as they may engage in some side activities under certain conditions, but must be ready to drive.[44] As for Level 4 (fully autonomous within limits), since the 2021 law allows no driver on board,[45] German law faces a new scenario to identify who is criminally liable if an uncrewed vehicle causes harm. If the cause was a pure system malfunction, with no reasonable human intervention possible, liability might shift to those responsible for the system's safety, potentially the manufacturer or the organization deploying the AV.[46] However, German criminal law does not readily attribute criminal liability to a corporation or software; it typically requires a natural person's guilt.[47]

France. France introduced explicit provisions in its Traffic Code and Criminal Code to address offenses committed by automated vehicles. Under these rules, when a driver activates an authorized automated driving system, they are exempt from criminal liability for standard traffic violations if the system is under control.[48] However, the human can be liable if they fail to take back control when the law or the system requires them to (e.g., if they ignore a police order to stop or a clear handover prompt), to ensure that drivers cannot use automation to escape responsibility when they should intervene.

---

43 Sadaf Fahim, "Criminal Liability of Artificial Intelligence," in *Ethico-Legal Aspect of AI-Driven Driverless Cars: Comparing Autonomous Vehicle Regulations in Germany, California, and India* (Singapore: Springer Nature, 2024), 89–127.

44 This refers to the Eighth Act amending the Road Traffic Act (Achtes Gesetz zur Änderung des Straßenverkehrsgesetzes), which entered into force on June 21, 2017 and is commonly referred to in English by the German Federal Ministry of Transport and Digital Infrastructure as the Act on Automated Driving. See: Marc Ruttloff, "New Legal Rules on Automated Driving," Gleiss Lutz, September 21, 2017, accessed February 23, 2026, https://www.gleisslutz.com/en/know-how/new-legal-rules-automated-driving.

45 Act Amending the Road Traffic Act and the Compulsory Insurance Act – Act on Autonomous Driving (Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren), which entered into force on July 28, 2021. Jenny Gesley, "Germany: Road Traffic Act Amendment Allows Driverless Vehicles on Public Roads," Library of Congress, August 9, 2021, accessed February 23, 2026, https://www.loc.gov/item/global-legal-monitor/2021-08-09/germany-road-traffic-act-amendment-allows-driverless-vehicles-on-public-roads/.

46 Tina Sever and Giuseppe Contissa, "Automated Driving Regulations – Where Are We Now?," *Transportation Research Interdisciplinary Perspectives* 24 (2024): 101033, https://doi.org/10.1016/j.trip.2024.101033.

47 There is an ongoing academic debate in Germany about applying concepts like "producer negligence" or corporate responsibility in such cases. See: Miriam C. Buiten, "Product Liability for Defective AI," *European Journal of Law and Economics* 57, no. 1 (2024): 239–73, https://doi.org/10.1007/s10657-024-09794-z.

48 In other words, if a Level 3 or 4 vehicle is driving itself within its legal operating domain, the human occupant will generally not receive a speeding ticket or a violation notice for things like failing to stop at a red light. The law recognizes that the human was not actually driving at that moment. See: Ozan Akyurek, Olivier Haas, and Philipp Werner, "France Plans on Adopting New Rules for Self-Driving Cars," Jones Day, April 2021, accessed February 23, 2026, https://www.jonesday.com/en/insights/2021/04/france-plans-on-adopting-new-rules-for-selfdriving-cars.

France's most groundbreaking step is making the vehicle manufacturer criminally liable for serious outcomes in autonomous mode. If, while self-driving in compliance with its approved conditions, an AV causes a death or injuries, the manufacturer of that AV can be prosecuted for involuntary manslaughter or causing injury.[49]

Netherlands. Under ordinary Dutch law, traffic offenses (speeding, failing to stop at a red light, causing an accident through negligence) presume a human driver in control. Since fully driverless operation is not generally allowed without a special permit, the permit conditions usually stipulate who is considered the responsible driver.[50] Thus, if a driver uses an AV in adaptive cruise or pilot mode and an offense occurs, Dutch police will treat the human behind the wheel as the responsible driver (automation is not an excuse for violating Article 5 of the Road Traffic Act, which requires drivers to behave safely).

4. Vietnamese Legal Framework

In the context of AVs, Vietnam's current legal framework lacks specific provisions tailored to self-driving technology. This section examines how Vietnam's laws on civil, administrative, and criminal liability would apply to AV-related incidents and contrasts them with approaches in the EU and Member States.

4.1. Civil Liability

4.1.1. Tort-Based Liability

Vietnam's Civil Code 2015 establishes general tort principles, alongside special rules for hazardous activities. Under Article 584, any person who harms another must compensate for the damage caused, unless a lawful exception applies.[51] In the context of traffic accidents, motor vehicles are classified as "sources of extreme danger," triggering a form of strict liability under Article 601 of the Civil Code.[52] This strict liability rule is coupled with a duty on owners to comply with safety regulations in operating and maintaining such dangerous vehicles. Ordinary, fault-based liability may still apply in situations falling outside the "extreme danger" category, but AVs are assumed to fall under the same strict liability regime as motor vehicles.

European legal systems have developed analogous doctrines. German law imposes strict liability on the keeper of a motor vehicle, which makes the keeper liable for any

49 Buiten, "Product Liability for Defective AI."

50 For example, during a driverless test, the remote operator or the company's safety officer might be designated as the responsible party under the law. If an AV test vehicle breaks a traffic rule, the authorities can impose penalties on the permit holder or the remote driver, as agreed in the exemption. See: William H. Widen and Marilyn Wolf, "Human Masters/Robot Servants: Highly Automated Vehicle Design, Intoxicated Drivers & Vicarious Liability," *Journal of Law and Mobility* (2025): 53, https://repository.law.umich.edu/jlm/vol2025/iss1/3.

51 Vietnamese Civil Code (No. 91/2015/QH13 of November 24, 2015), see: https://www.wipo.int/wipolex/en/legislation/details/17200.

52 The regulation provides that the owner (or person to whom the owner has transferred use) of a motorized vehicle must compensate for damage caused by the vehicle, even absent fault, subject only to narrow exceptions (such as the victim's sole intentional fault or force majeure). See: https://www.wipo.int/wipolex/en/legislation/details/17200.

damage caused by the vehicle's operation, "irrespective of any fault."[53] As under Vietnamese law, the German keeper's liability covers even accidents not involving driver error, embodying the concept that the vehicle owner bears the operational risk (*Betriebsgefahr*) related to the car. France's 1985 *Loi Badinter* on traffic accidents created a victim-friendly regime, since motor vehicle operators (and their insurers) are broadly liable towards injured persons (especially pedestrians and passengers), regardless of fault, with limited exceptions for truly unforeseeable circumstances or intentional fault on the part of the victim.[54] Similarly, the Netherlands protects road accident victims through Article 185 of its Road Traffic Act (*Wegenverkeerswet*), which imposes strict liability on motorized vehicle drivers for collisions with non-motorized users.[55]

Despite their common foundation, there are nuanced divergences. Vietnam's strict liability for sources of extreme danger applies to any harm caused by a motor vehicle, whether to other road users or property, and the only exceptions are narrow lines of defense. German law likewise only makes an exception for the keeper in the case of force majeure, or if the injured party wholly caused the incident. Dutch law's strict liability, by contrast, is chiefly limited to protecting non-motorized victims; collisions exclusively between cars fall back on ordinary negligence rules. French law focuses on personal injury, leaving property damage to general tort principles. Another difference is how an AV's self-driving system is treated; Vietnam's doctrine, which does not yet differentiate between human-driven and autonomous modes, could draw from the European experience, for instance, clarifying the liability of an AV operator versus the vehicle's manufacturer when an algorithm, rather than a person, is doing the driving.

4.1.2. Product Liability

Vietnam's current law provides injured parties with recourse under both general tort and consumer protection regimes for defective products. The Civil Code 2015 establishes a general principle that producers or sellers must compensate consumers for damage caused by substandard goods, in terms of safety or quality.[56] More specifically, Article 34 of the Vietnam Law on Protection of Consumer Rights 2023 (LPCR 2023) introduced a regime akin to strict product liability.[57] Then, if an AV's automated driving system or component is defective and causes damage, the manufacturer (or other responsible trader) is strictly liable towards the injured consumer, without the need to prove negligence. The LPCR 2023 broadly defines a "defective" product as one that does not ensure safety

53 Von Bodungen and Steege, "Liability for Automated and Autonomous Driving in Germany."

54 Knetsch, "La voiture autonome face au droit."

55 A Dutch motorist must compensate a pedestrian or cyclist for injuries in almost all cases, barring extraordinary circumstances beyond the driver's control. Even if a non-motorized victim was partly at fault, Dutch law mandates that the driver of the car bear at least 50% of the loss, and 100% if the victim is a child under 14. Wrzesniowska, "Can AI Make a Case? AI Vs. Lawyer in the Dutch Legal Context."

56 Article 608 of the Vietnamese Civil Code.

57 Businesses are liable for damages where products and goods with defects, supplied by them, cause damage to the life, health, or property of consumers, even when such organizations or individuals are not aware of, or at fault for, the defects arising. Article 34 of the Vietnamese Law on Protection of Consumer Rights (No. 19/2023/QH15 of June 20, 2023). See: https://luatvietnam.vn/thuong-mai/luat-bao-ve-quyen-loi-nguoi-tieu-dung-2023-so-19-2023-qh15-259732-d1.html.

for consumers and poses a risk to life, health, or property, even if the product was manufactured in accordance with proper technical standards.[58] In the AV context, this means a design bug in the vehicle's collision-avoidance algorithm, a sensor manufacturing fault, or a failure to warn users of the AV's operational limits. These could each render the vehicle "defective" under the law. Once such a defect occurs, Article 34(1) mandates that the responsible business compensate any consumer for injury or property damage caused by the AV, irrespective of the business's knowledge or care.

The law covers not only the vehicle's manufacturer, but also the importer and any entity that promotes the product as its own brand, acts as an intermediary in the distribution chain, and directly supplies the product to consumers.[59] Multiple parties can also be jointly liable if their combined actions caused the defect. This structure closely mirrors the European approach, when, under the EU Product Liability Directive of 1985 (now revised in 2024), the producer (including manufacturers, any entity that promotes the product as its own brand, and importers) is strictly liable. If the producer is unknown, the supplier can be held liable.[60] The new EU Directive 2024/2853 explicitly extends liability to cover certain service providers in the supply chain, such as fulfillment service providers and online marketplaces, for similar reasons.

One important divergence lies in who is protected by Vietnam's product liability rules. Article 34 of the LPCR 2023 covers only "consumers," i.e., persons who purchase or use goods for personal or household purposes (non-commercial use).[61] By contrast, European product liability regimes are not limited to consumer plaintiffs, since any injured person can sue the producer for damages caused by a defective product, regardless of consumer status.[62] This divergence may prompt future Vietnamese reforms to broaden protection beyond the consumer category, especially as AVs blur the line between product users and third parties on the road.

Although Vietnam imposes strict liability, Article 35 of the 2023 law provides for several key exemptions that echo those in European law. Most prominently, Vietnam adopted the development risk defense. This means that a manufacturer or supplier can avoid liability if it proves that the product's defect could not have been detected with the level of science and technology available worldwide up to the time the product caused the damage. This mirrors the defense under the EU's 1985 Product Liability Directive,

58 Article 3(2) of LPCR 2023.

59 Article 34(2) of the LPRC 2023.

60 For example, French law defines "manufacturer" to include anyone who presents themselves as the producer or importer, and allows claimants to sue a seller or importer if the actual producer is unidentified. Similarly, German and Dutch laws implemented the EU directive with identical coverage. See also: Morgan, "Chapter 1: Tort Liability and Autonomous Systems Accidents."

61 Thus, if an autonomous vehicle's defect injures a bystander or a business user (for instance, a rideshare driver using an AV for commercial purposes), it is unclear if they qualify as "consumers" entitled to a claim under this law. They may instead have to rely on general tort provisions in the Civil Code (which require proof of fault).

62 The EU's original directive and its national implementations (e.g., Code Civil Article 1245 in France, ProdHaftG in Germany) cover all persons who suffer injury or property damage (excluding property used for business), without requiring that the victim bought or used the product as a consumer.

which allows producers to escape liability for unknown risks.[63] In the AV context, this defense could be invoked if, for example, an advanced neural-network driving system made an unpredictable error that no existing testing method could have identified.

Aside from development risks, Article 35(2) of the LPCR 2023 introduces a defense akin to contributory fault; if the business has fully complied with its duties under Articles 32–33 (e.g., recalling the product and warning consumers in a timely fashion), and yet the consumer knowingly ignores the warnings and continues to use the defective product, then the business is exempt from liability. While the EU directive does not list consumer misuse as a formal defense, national laws (and general principles of tort) provide that damages can be reduced if the injured party negligently contributed to the damage.[64]

4.2. Administrative Liability

The newly enacted Law on Road Traffic Safety and Order (effective 2025) defines "smart vehicles" as motor vehicles capable of partial or complete automation, classified into five levels.[65] Under this law, even vehicles with advanced driver-assistance features (SAE Levels 1–3) are considered "smart" and special operational licenses must be obtained, unlike in the case of conventional cars. By contrast, fully self-driving vehicles (Levels 4–5) are not yet broadly permitted; the Ministry of Public Security has proposed that any deployment of Level 4–5 AVs be tightly restricted and subject to special permits, given Vietnam's current road and traffic conditions.[66] Existing Vietnamese law imposes various duties on drivers and vehicle owners to ensure traffic safety. The regulatory logic is one of personal responsibility, since the onus is on the individual behind the wheel (or the owner, in some cases) to comply with technical and safety standards.[67] However, these rules evolved before the advent of self-driving technology. There is, for example, no legal obligation in Vietnam for a vehicle maker to ensure software updates are installed, nor any concept of a "remote operator" or "technical supervisor."

By contrast, under Germany's 2021 Autonomous Driving Act, Level 4 operation depends on defined operational domains and the appointment of a (potentially remote) technical supervisor, supported by enhanced insurance and stringent system safety

63 France, Germany, and the Netherlands each permit this defense. Germany's Product Liability Act § 1(3) explicitly excludes liability for defects not discoverable given the scientific/technical knowledge at the time of sale).

64 For example, under French civil law, if a claimant knowingly uses a recalled dangerous product, the court could find a causal link broken or the claimant predominantly at fault, defeating the claim. See also: Akyurek, Haas, and Werner, "France to Adopt New Rules for Self-Driving Cars."

65 Vietnamese Law on Road Traffic Safety and Order (No. 36/2024/QH15 of June 27, 2024), see: https://thuvienphapluat.vn/van-ban/EN/Giao-thong-Van-tai/Law-36-2024-QH15-Road-Traffic-Order-and-Safety/620124/tieng-anh.aspx.

66 "Fully Autonomous Cars Not Yet Suitable for Vietnam's Road Conditions: Ministry," Vietnam+ (VietnamPlus), May 8, 2025, accessed February 23, 2026, https://en.vietnamplus.vn/fully-autonomous-cars-not-yet-suitable-for-vietnams-road-conditions-ministry-post323969.vnp.

67 For instance, operating a vehicle that fails to meet required technical inspection standards can result in sanctions against the driver or owner. Other parties can also be held accountable under specific provisions (e.g., inspection officials who falsify roadworthiness results, or companies that assemble vehicles without authorization).

requirements (including minimal risk behavior). The Netherlands has pursued a permit-and-exemption model, administered by the RDW, for controlled trials, typically requiring a designated remote controller. France, through its 2021 framework, has integrated AVs into road traffic administration by specifying when the ADS is legally in control, and by placing compliance, data access, and user notification obligations on manufacturers/operators.

Both Vietnam and the European systems recognize administrative law as a vital tool for preventing accidents. However, their doctrinal approaches diverge in allocating responsibility for AV safety. Vietnam's framework remains driver-centric and reactive, focused on punishment for traffic violations after they occur, premised on a human's duty to control the vehicle. In contrast, the European approaches increasingly blend *ex ante* oversight with shared responsibility among the stakeholders. They impose specific legal obligations on manufacturers and vehicle operators with regard to vehicle software, data reporting, and ensuring safe operation, and create new actor roles (technical supervisors, in-use safety regulators) to govern autonomous driving in real time. Vietnam may draw on European experience by instituting measures such as special AV operating permits, mandatory safety self-assessments by manufacturers, and mechanisms to sanction lapses in an AV's performance.

4.3. Criminal Liability

Under the Vietnamese Penal Code, traffic accidents may result in criminal prosecution if individuals violate road safety rules or are grossly negligent.[68] Crucially, however, these offenses presume that a human actor has breached a duty of care behind the wheel. Corporate criminal liability in Vietnam is a relatively new and limited concept. The Penal Code allows legal entities to be prosecuted for certain economic or environmental crimes,[69] but not for traffic offenses or negligent homicide. Thus, under the current law, if an autonomous vehicle operating without active human control were to cause a serious accident, it is unclear who (if anyone) could be criminally prosecuted.

European legal systems are beginning to grapple with the same challenge, and their solutions highlight different regulatory logic. One approach is to shift criminal responsibility from the individual to the entity that effectively "controls" the risk in autonomous mode. Under France's 2021 AV legislation, when a vehicle is driving itself in an authorized autonomous mode, the human user is immune from criminal liability for traffic offenses, and any harm caused is attributable instead to the vehicle's manufacturer

[68] For example, a human driver who causes a fatal crash by speeding or failing to stop at a red light can be charged with violating traffic safety regulations, or even involuntary manslaughter, depending on the circumstances. Vehicle owners or others might be liable as accomplices (for instance, allowing an unqualified person to drive or failing to fix known vehicular defects). See Article 260 of the Vietnamese Law on the Penal Code (No. 100/2015/QH13) amended by Law No. 12/2017/QH14 of June 20, 2017, see: https://luatvietnam.vn/hinh-su/bo-luat-hinh-su-sua-doi-2017-115503-d1.html.

[69] Nguyen Hung, Mai Van Thang, and Tran Thu Hanh, "The Criminal Liability of Commercial Legal Entities in the Current Criminal Code of Vietnam," *PRAWO i WIĘŹ* 40, no. 2 (2022): 185–98, https://doi.org/10.36128/priw.vi40.398.

or system provider.[70] At the same time, French law does not give human users *carte blanche*. If the person in the driver's seat fails to take over manual control despite a legal obligation to do so (for example, ignoring a police officer's order or a clear handover prompt from the vehicle),[71] then that individual can still be held criminally liable for the consequences, in the same way as a conventional driver. Germany and the Netherlands, by contrast, have not fundamentally changed their criminal laws for AVs. German law still requires a natural person to be at fault for a traffic offense or vehicular homicide, and it has no provision allowing prosecutors to impute a road accident crime to an autonomous system or a manufacturer in the absence of human wrongdoing.[72] The Netherlands similarly treats the human as the responsible driver in any AV operation, relying on permit conditions or existing rules to identify an individual (such as a remote operator) who can be blamed for violations.[73]

In the situation in Vietnam, if a truly autonomous vehicle were tested or operated, and a crash occurred, prosecutors would likely resort to existing statutes, perhaps charging a human safety operator for negligence, or an owner for allowing an unsafe vehicle to circulate.[74] However, if an accident is caused solely by an AV's independent action (e.g., a Level 4 test car swerving and hitting a pedestrian due to a sensor algorithm flaw), the attribution of criminal fault under current law is highly problematic. One suggestion is to expand corporate criminal liability to cover traffic-related offenses involving autonomous systems, for example, adding a provision that a "crime committed by an AI driving system" can lead to criminal responsibility of the legal entity that programmed or deployed it.[75] Another recommendation is to create specific offenses (or expand existing ones) to hold manufacturers accountable for gross negligence in the design or deployment of self-driving technology, such as releasing an unsafe vehicle that causes a fatal accident.

5. Conclusion

This article has argued that autonomous vehicles should be analyzed not as a single liability puzzle, but as a liability architecture problem spanning civil compensation, administrative safety governance, and criminal attribution. The comparative research shows that the EU contribution is best understood as a multi-level settlement, rather than a unified AV liability code. On the EU scale, the system prioritizes victim protection through insurance-first mechanisms and the modernization of product liability for software-enabled

70 Akyurek, Haas, and Werner, "France to Adopt New Rules for Self-Driving Cars."

71 Ibid.

72 Thus, if a Level 4 vehicle in Germany crashes due to a software error, with no human misconduct, criminal law may find no one to hold culpable. Galassi et al., "Safety Approval of Automated Vehicles in the EU."

73 While Dutch law does allow corporate criminal liability in principle, it has not yet been applied to an AV-related incident. Wrzesniowska, "Can AI Make a Case? AI Vs. Lawyer in the Dutch Legal Context."

74 The Vietnamese Penal Code does criminalize the act of letting someone use a vehicle that does not meet safety standards (Article 262).

75 Hung, Thang, and Hanh, "The Criminal Liability of Commercial Legal Entities in the Current Criminal Code of Vietnam."

harms, while Member States supply the legally salient roles and evidence tools that make allocation workable in practice. Germany, France, and the Netherlands demonstrate that role definitions, domain restrictions, event data logging, and disclosure pathways do not merely supplement civil liability; they enable it to function under conditions of black-box decision-making and mixed causation.

When viewed through the same architecture, Vietnam's framework is not an empty field. Vietnam already exhibits a strong commitment to rapid victim compensation through strict risk doctrines for hazardous vehicles, and has strengthened product responsibility through the LPCR 2023. The main challenge is fit: evidentiary access, cyber-incident attribution, and the delineation of roles in higher automation. A coherent, Vietnam-adapted direction therefore preserves compensation-first logic while structuring recourse, embeds update/cybersecurity and data logging duties in administrative law, and keeps criminal liability calibrated and exceptional. In this sense, comparative analysis is not a hierarchy of advanced and lagging systems, but a way to identify design measures that can be selectively translated while respecting Vietnam's own doctrinal commitments.

Funding: This research is funded by Vietnam National University Ho Chi Minh City (VNU-HCM) under grant number DM2024-34-02.

References

Akyurek, Ozan, Olivier Haas, and Philipp Werner. "France Plans on Adopting New Rules for Self-Driving Cars." Jones Day, April 2021. Accessed February 23, 2026. https://www.jonesday.com/en/insights/2021/04/france-plans-on-adopting-new-rules-for-selfdriving-cars.

Buiten, Miriam C. "Product Liability for Defective AI." *European Journal of Law and Economics* 57, no. 1 (2024): 239–73. https://doi.org/10.1007/s10657-024-09794-z.

Cabral, Tiago Sérgio. "Liability and Artificial Intelligence in the EU: Assessing the Adequacy of the Current Product Liability Directive." *Maastricht Journal of European and Comparative Law* 27, no. 5 (2020): 615–35. https://doi.org/10.1177/1023263X20948689.

Dziadkiewicz, Marcin. "Technological Innovations in Transportation: Law and Practice." In *The Use of Information and Communication Technologies (ICT) in the Management of the Innovative and Smart City*, edited by Judyta Kabus, Luiza Piersiala, and Michał Dziadkiewicz, 64–99. Boca Raton: CRC Press. 2024.

Evas, Tatjana. "A Common EU Approach to Liability Rules and Insurance for Connected and Autonomous Vehicles: European Added Value Assessment: Accompanying the European Parliament's Legislative Own Initiative Report." European Parliamentary Research Service, February 2018. Accessed February 23, 2026. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2018)615635.

Fahim, Sadaf. "Criminal Liability of Artificial Intelligence." In *Ethico-Legal Aspect of AI-Driven Driverless Cars: Comparing Autonomous Vehicle Regulations in Germany, California, and India*, 89–127. Singapore: Springer Nature, 2024.

Galassi, Maria Cristina, Antony Lagrange, Biagio Ciuffo, Ricardo Suarez Bertoa, Sandor Vass, Konstantinos Mattas, Riccardo Donà, and Calogero Sollima. "Safety Approval of Automated Vehicles

in the EU: Moving Beyond Highway Applications." *Transportation Research Procedia* 72 (2023): 4396–403. https://doi.org/10.1016/j.trpro.2023.11.328.

Gerber, Michael A., Ronald Schroeter, and Bonnie Ho. "A Human Factors Perspective on How to Keep SAE Level 3 Conditional Automated Driving Safe." *Transportation Research Interdisciplinary Perspectives* 22 (2023): 100959. https://doi.org/10.1016/j.trip.2023.100959.

Gesley, Jenny. "Germany: Road Traffic Act Amendment Allows Driverless Vehicles on Public Roads." Library of Congress, August 9, 2021. Accessed February 23, 2026. https://www.loc.gov/item/global-legal-monitor/2021-08-09/germany-road-traffic-act-amendment-allows-driverless-vehicles-on-public-roads/.

Hopkins, Debbie, and Tim Schwanen. "Talking about Automated Vehicles: What Do Levels of Automation Do?." *Technology in Society* 64 (2021): 101488. https://doi.org/10.1016/j.techsoc.2020.101488.

Hung, Nguyen, Mai Van Thang, and Tran Thu Hanh. "The Criminal Liability of Commercial Legal Entities in the Current Criminal Code of Vietnam." *PRAWO i WIĘŹ* 40, no. 2 (2022): 185–98. https://doi.org/10.36128/priw.vi40.398.

Kerrigan, Charles, Sean Musch, and Michael Borrelli. "The EU AI Act." In *Artificial Intelligence*, edited by Charles Kerrigan, 178–239. Cheltenham: Edward Elgar Publishing, 2025. https://doi.org/10.4337/9781035334353.00020.

Knetsch, Jonas. "La voiture autonome face au droit: les réponses en droit positif et en droit prospectif (Regards d'aujourd'hui vers le futur ?): Rapport français." In *Autonomous Vehicles and the Law*, edited by Gilles Pillet, 158–87. Leiden: Brill–Nijhoff, 2025.

Kouroutakis, Antonios E. "Autonomous Vehicles: Regulatory Challenges and the Response from Germany and UK." *Mitchell Hamline Law Review* 46, no. 5 (2020): 1103. https://open.mitchellhamline.edu/mhlr/vol46/iss5/3.

Ministerie van Infrastructuur en Waterstaat. "Mobility, Public Transport and Road Safety: Self-Driving Vehicles," 2025. Accessed February 23, 2026. https://www.government.nl/topics/mobility-public-transport-and-road-safety/self-driving-vehicles.

Morgan, Phillip. "Chapter 1: Tort Liability and Autonomous Systems Accidents – Challenges and Future Developments." In *Tort Liability and Autonomous Systems Accidents: Common Law and Civil Law Perspectives*, edited by Phillip Morgan, 1–26. Northampton: Edward Elgar Publishing, 2023.

Polad, Didem. "Liability Perspective for Users of Autonomous Vehicles in the EU." RAILS – Blog, April 15, 2024. Accessed February 23, 2026. https://blog.ai-laws.org/liability-perspective-for-users-of-autonomous-vehicles-in-the-eu/.

Ruttloff, Marc. "New Legal Rules on Automated Driving." Gleiss Lutz, September 21, 2017. Accessed February 23, 2026. https://www.gleisslutz.com/en/news-events/know-how/new-legal-rules-automated-driving.

Schellekens, Maurice. "Self-Driving Cars and the Chilling Effect of Liability Law." *Computer Law & Security Review* 31, no. 4 (2015): 506–17. https://doi.org/10.1016/j.clsr.2015.05.012.

Sever, Tina, and Giuseppe Contissa. "Automated Driving Regulations – Where Are We Now?." *Transportation Research Interdisciplinary Perspectives* 24 (2024): 101033. https://doi.org/10.1016/j.trip.2024.101033.

STRMTG. "The French Regulatory Framework for Automated Road Transport Systems (ARTS) Has Been Published." STRMTG Web Site, October 4, 2022. Accessed February 23, 2026. https://www.strmtg.developpement-durable.gouv.fr/en/the-french-regulatory-framework-for-automated-road-a167.html.

Tennant, Chris, Jack Stilgoe, Sandra Vucevic, and Sally Stares. "Public Anticipations of Self-Driving Vehicles in the UK and US." *Mobilities* 20, no. 2 (2025): 292–309. https://doi.org/10.1080/17450101.2024.2325386.

Tjong Tjin Tai, Eric. "Civil Liability for Self-Driving Cars in Dutch Law." In *Autonomous Vehicles and Civil Liability in a Global Perspective*, edited by Hans Steege, Ilaria Amelia Caggiano, Maria Cristina Gaeta, and Benjamin Von Bodungen, 385–403. Cham: Springer, 2024.

Vanetta, Sara, Christian M. Theissen, and Isabelle Peltier. "Navigating Product Liability in High-Security Sectors: Addressing AI-Driven Risks under German and European Law." White & Case LLP, December 16, 2025. Accessed February 23, 2026. https://www.whitecase.com/insight-alert/navigating-product-liability-high-security-sectors-addressing-ai-driven-risks-under.

Vietnam+ (VietnamPlus). "Fully Autonomous Cars Not Yet Suitable for Vietnam's Road Conditions: Ministry," May 8, 2025. Accessed February 23, 2026. https://en.vietnamplus.vn/fully-autonomous-cars-not-yet-suitable-for-vietnams-road-conditions-ministry-post323969.vnp.

Von Bodungen, Benjamin, and Hans Steege. "Liability for Automated and Autonomous Driving in Germany." In *Autonomous Vehicles and Civil Liability in a Global Perspective: Liability Law Study across the World in Relation to SAE J3016 Standard for Driving Automation*, edited by Hans Steege, Ilaria Amelia Caggiano, Maria Cristina Gaeta, and Benjamin von Bodungen, 279–320. Cham: Springer, 2024.

Van Wees, K.A.P.C. "Civil Liability for Autonomous Vehicles in the Netherlands." In *Autonomous Vehicles and the Law: A Revolution through the Prism of Civil Liability*, edited by Gilles Pillet, 289–330. Leiden: Brill, 2025. https://doi.org/10.1163/9789004711891_009.

Widen, William H., and Marilyn Wolf. "Human Masters/Robot Servants: Highly Automated Vehicle Design, Intoxicated Drivers & Vicarious Liability." *Journal of Law and Mobility* (2025): 53–92. https://repository.law.umich.edu/jlm/vol2025/iss1/3.

Wrzesniowska, Lena. "Can AI Make a Case? AI Vs. Lawyer in the Dutch Legal Context." *International Journal of Law, Ethics & Technology* 4, no. 3 (2024): 1–49.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 153–167
https://doi.org/10.31743/recl.19516
Received: 19 January 2026 | Accepted: 23 February 2026 | Published: 31 March 2026

Resilience in Labor Regulation: Evaluating Serbia's Post-Pandemic Occupational Safety and Health Reform

Sanja Zlatanović

PhD, Senior Research Fellow, Institute of Social Sciences, Belgrade, Serbia; correspondence address: Kraljice Natalije 45, Belgrade, Serbia; e-mail: sanjazlatanovic1@gmail.com
https://orcid.org/0000-0001-7753-0876

Anđelija Stevanović

LLM, Research Assistant, Institute of Social Sciences, Belgrade, Serbia & Junior Researcher, Central European Academy, Budapest, Hungary; correspondence address: Kraljice Natalije 45, Belgrade, Serbia; e-mail: andjelija.stevanovic21@gmail.com
https://orcid.org/0009-0002-3157-515X

Abstract: The COVID-19 pandemic exposed fundamental weaknesses in labor law systems worldwide, revealing their limited capacity to manage public health crises. In Serbia, it highlighted longstanding gaps in regulations on remote work, occupational safety and health (OSH), and the continuity of labor rights during emergencies. This paper examines the post-pandemic evolution of Serbian labor law, focusing on the 2023 Occupational Safety and Health Act, and evaluates its effectiveness in addressing lessons from the crisis. Although the 2023 OSH Act updated certain safety standards, it largely neglects mental health protection and the systematic management of psychosocial risks – issues increasingly recognized as central to occupational safety internationally. The law remains focused on physical risks, offering limited provisions for stress prevention, psychosocial well-being, or emergency support mechanisms. Temporary pandemic measures, such as flexible work arrangements, were not codified, leaving gaps in social dialogue, employer obligations, and protections for workers' rights. The study concludes that Serbia's labor law remains structurally unprepared for future public health emergencies. Enhancing resilience requires integrating psychosocial risk management into OSH regulations, formally recognizing mental health as a core aspect of workplace safety and establishing robust legal mechanisms for emergency labor governance. These reforms are essential to safeguard workers' rights and ensure safe, inclusive, and adaptable work environments during societal disruptions.

Keywords: labor law, OSH, mental health, resilience, Serbia normative framework

1. Introduction

The COVID-19 pandemic exposed persistent regulatory fragilities within labor law systems across jurisdictions, while simultaneously revealing the structural vulnerabilities of health care systems that were unprepared to manage systemic public health risks. From a critical theoretical perspective, these parallel failures underscore the limits of labor law's traditionally fragmented and reactive regulatory model, which continues to treat occupational safety and health (OSH) risks as isolated (potential) workplace hazards rather than as manifestations of broader social, organizational, and institutional risk structures. In conditions characteristic of late modern "risk societies," the pandemic demonstrated how the inadequate integration of labor law, OSH regulation, and public health governance exacerbated workers' exposure to both physical and psychosocial harms. This

ISSN 2545-384X (Online)

disjunction was particularly visible in the insufficient legal recognition of emerging and cumulative risks – such as mental health strain, moral injury, and precariousness intensified by crisis management measures – thereby highlighting labor law's diminished capacity to function as an effective instrument of collective risk prevention and social protection in the face of systemic shocks.

Additionally, these regulatory shortcomings directly challenge the normative foundations of decent work, which presuppose not only safe and healthy working conditions, but also institutional coherence capable of safeguarding workers' dignity and well-being in times of systemic crisis. The pandemic revealed that fragmented labor and health governance undermine social sustainability by shifting the costs of social risk onto workers, particularly those in precarious or essential roles. In this sense, strengthening the integration between labor law, OSH, and public health systems emerges as a precondition for realizing decent work as a sustainable social objective rather than a merely aspirational standard.

In Serbia, pre-existing labor regulations were unprepared to address challenges arising from remote work, continuity of labor rights, and psychosocial well-being during prolonged crises. These shortcomings prompted legislative reform, culminating in the Law on Occupational Safety and Health (35/2023) ("OSH Act 2023"), which seeks to modernize workplace safety standards and align domestic law with European and international frameworks. While the Act strengthens procedural aspects of occupational safety, critiques highlight its continued emphasis on physical hazards and the marginalization of mental health and psychosocial risk management, despite growing recognition that mental well-being is a central component of decent work and sustainable labor governance.[1]

This paper evaluates Serbia's post-pandemic OSH reforms using legal-theoretical and normative methods, combining doctrinal legal analysis with a critical assessment of comparative best-practice approaches. It examines the conceptualization of psychosocial risks within OSH law through an interdisciplinary lens that integrates resilience management theory with legal analysis, assesses Serbia's alignment with European standards, and critically evaluates the resilience of the national OSH regulatory framework – specifically, its capacity to anticipate, absorb, adapt to, and recover from systemic disruptions, including pandemics and rapid digitalization.

2. Towards Integration of Psychosocial Risk Management and Resilience in OSH Law – Conceptual Issues

According to the prevailing view, psychosocial risks constitute a category of occupational hazards stemming from the design, organization, and social context of work, with

[1] Ryan D. Duffy et al., "Linking Decent Work with Physical and Mental Health: A Psychology of Working Perspective," *Journal of Vocational Behavior* 112 (2019): 384–95, https://doi.org/10.1016/j.jvb.2019.05.002; "Mental Health at Work: Policy Brief," International Labor Organization and World Health Organization, 2022, accessed December 10, 2025, https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40ed_protect/%40protrav/%40safework/documents/publication/wcms_856976.pdf.

significant consequences for both psychological and physical health.[2] In line with this understanding, the European Agency for Safety and Health at Work (EU-OSHA) has emphasized that the COVID-19 pandemic significantly exacerbated psychosocial risks, intensifying pre-existing challenges and bringing workplace mental health to the forefront of occupational safety debates.[3] Psychosocial risks predominantly include excessive workload, role ambiguity, lack of autonomy, inadequate social support, and workplace harassment, reflecting systemic conditions rather than isolated incidents. When left unaddressed, psychosocial hazards can undermine organizational functioning, reduce productivity, and compromise overall workforce health and well-being.[4]

Although the terms "psychosocial risks," "psychosocial factors," and "psychosocial hazards" are often used interchangeably in the literature, Leka and Cox clarify that "psychosocial hazards" refer to the psychosocial factors, i.e., risks defined by the ILO, all of which are intrinsically tied to work organization and management.[5] Recognizing this distinction is essential for labor law and occupational safety, as it underscores employers' responsibility to address organizational factors that affect employees' mental health. In a narrower sense, psychosocial risks may be understood as organizational and managerial factors inherent in work design and organization. In contrast, psychosocial hazards represent their concrete manifestations and adverse consequences, which are addressed through the application of OSH standards and labor law protections.

Addressing both risks and hazards thus aligns with the ILO's concept of "decent work" and EU soft law on workplace mental health, emphasizing the integration of psychosocial risk assessment and management into legal and organizational frameworks. Additionally, recognizing this distinction is crucial for labor law and occupational safety frameworks, as it underscores the need for employers to address organizational and management-related factors that can affect employees' mental health and well-being. From a labor law perspective, the recognition of psychosocial risks imposes clear obligations on employers to identify, prevent, and mitigate these hazards, thereby ensuring compliance with the duty of care principle and reducing potential legal liability for employee harm.

Psychosocial risks are primarily examined within organizational management and occupational psychology, where they are analyzed in terms of work design, organizational structures, and social relationships at work, and their impacts on employee well-being are subsequently linked to broader working conditions and occupational health outcomes.[6]

---

2 "Psychosocial Risks," European Foundation for the Improvement of Living and Working Conditions (Eurofound), 2025, accessed December 5, 2025, https://www.eurofound.europa.eu/en/topics/psychosocial-risks.

3 "Strategies and Legislation on Psychosocial Risks in Six European Countries: Policy Brief," European Agency for Safety and Health at Work (EU-OSHA), 2025, accessed January 8, 2026, https://osha.europa.eu/en/publications/strategies-and-legislation-psychosocial-risks-six-european-countries.

4 Paul A. Schulte et al., "An Urgent Call to Address Work-Related Psychosocial Hazards and Improve Worker Well-Being," *American Journal of Industrial Medicine* 67, no. 6 (2024): 499–514, https://doi.org/10.1002/ajim.23583.

5 Stavroula Leka and Tom Cox, eds., *The European Framework for Psychosocial Risk management (PRIMA-EF)* (Nottingham: Institute of Work, Health and Organization, 2008), 5.

6 Eurofound and EU-OSHA, *Psychosocial Risks in Europe: Prevalence and Strategies for Prevention* (Luxembourg: Publications Office of the European Union, 2014).

In contrast, labor law is still grappling with the concept, which remains vague in both legal definition and in employers' practical application. This lack of precise legal recognition means that obligations to prevent or mitigate psychosocial risks are often unclear, leaving gaps in enforcement and compliance. As a result, while organizations may implement management-driven interventions to address stressors and promote well-being, the absence of robust legal frameworks can limit accountability, weaken employee protections, and hinder the integration of psychosocial risk management into formal OSH systems. Clarifying the legal status of psychosocial risks is therefore essential to align organizational practices with enforceable labor law duties and to ensure comprehensive protection of workers' mental health and well-being.

Thus, despite growing recognition of workplace mental health, labor law theory, legislation, and practice still lack clear definitions of psychosocial risks and hazards. This ambiguity often leads employers to overlook their integration into OSH systems. On the other hand, international bodies, notably the WHO and ILO, emphasize that mental health deserves protection equal to that of physical health under the right to health. In the post-pandemic era, rigorous legal and theoretical clarification of psychosocial risks has become indispensable for the effectiveness of OSH frameworks and for advancing broader public health objectives. The pandemic demonstrated that intensified workloads, extended working hours, and emergency forms of work organization during crises had a disproportionate impact on workers' mental health and well-being, revealing higher levels of depression among women, younger employees, and individuals whose quality of life was adversely affected by the coronavirus.[7] Consistent with evidence that intensified workloads, extended hours, and emergency work organization during the pandemic disproportionately harmed workers' mental health, the systematic review by Rossi *et al.* (2023) found that burnout was widespread among workers – especially in predominantly female healthcare samples – and that maladaptive coping styles, which may exacerbate stress under high job demands, were associated with higher burnout levels, while adaptive coping was protective, with some coping outcomes varying by gender,[8] suggesting that pandemic work conditions and individual coping strategies jointly influenced psychological distress. Overall, these findings expose structural limitations in existing regulatory frameworks and underscore the need to reconceptualize psychosocial risk prevention as an integral component of resilient labor law and the promotion of decent work to mitigate psychosocial hazards effectively.

In response, scholars have increasingly sought to distinguish between mental health at work as a labor law issue and psychosocial risk management as a traditional organizational management concern. Accordingly, Lerouge argues that legal discussions on workplace mental health and psychosocial risks require a clear conceptual separation, as these terms are often conflated despite their distinct legal and practical implications.

---

7 Didem Rodoplu Şahin et al., "The Effect of COVID-19 on Employees' Mental Health," *Scientific Reports* 12, 15067, (2022), https://doi.org/10.1038/s41598-022-18692-w.

8 Maria Francesca Rossi et al., "Coping with Burnout and the Impact of the COVID-19 Pandemic on Workers' Mental Health: A Systematic Review," *Frontiers in Psychiatry* 14, 1139260 (2023), https://doi.org/10.3389/fpsyt.2023.1139260.

The author emphasizes that "mental health in the workplace" broadly refers to the overall psychological well-being of workers. In contrast, psychosocial risks denote specific, work-related conditions – such as stressors arising from job design or organizational structure – that can undermine well-being.[9] Clarifying these concepts is essential for effective legal regulation and policy-making, as it helps protect workers, delineate employers' responsibilities, and guide targeted labor law interventions. The author situates this discussion within the context of recent EU-level initiatives and pressures to develop legal frameworks to address these issues.

As a continuation of recent legal developments and scholarly discussions within a legal-theoretical framework, on the other side, the integration of psychosocial risks management practice into the workplace represents a paradigmatic shift from traditional, reactive approaches – centered on physical safety and hazard elimination – toward proactive, principles-based governance that aligns with the broader "concept of resilience." While the prevailing view in the organization science literature holds that there is no universally agreed-upon definition of resilience, it is often described as multifactorial, multilevel, and multidimensional, encompassing principles of anticipation, response, learning, adaptation and recovery.[10] In legal terms, resilience thus refers to the capacity of regulatory systems to anticipate, absorb, adapt to, and recover from disruptive events, while maintaining core protections and safeguarding fundamental workers' rights.

While resilience has traditionally been studied in psychology as an individual mechanism, it is important, in this context, to highlight the work of Calado, Capucha, and Wódz, who offer a critical "conceptualization of social resilience" that extends beyond individual coping. Their analysis demonstrates how systemic shocks – such as the financial crisis and, similarly, "public health crises like pandemics" – can trigger structural reconfigurations of labor relations in Europe, reshaping labor market institutions, power dynamics, and the distribution of resources across national contexts.[11] The authors' comparative analysis of Portugal, Poland, and Ireland demonstrates that resilience is not merely a passive recovery to pre-crisis conditions, but a dynamic process in which labor relations are transformed and, in some cases, liberalized, highlighting the centrality of institutional rules and power dynamics in shaping post-crisis labor regimes.[12]

This institutional perspective aligns with broader theoretical work on social resilience that emphasizes the importance of rules, resources, and power relations in understanding how social systems adapt to shocks, suggesting that resilience cannot be abstracted from the socio-economic and legal frameworks within which labor markets

---

9 Loïc Lerouge, "The Concepts of 'Mental Health in the Workplace' and 'Psychosocial Risks': A Clarification from a Legal Perspective," *European Labour Law Journal* 16, no. 3 (2025): 377–83, https://doi.org/10.1177/20319525251336018.

10 Royce Francis and Behailu Bekera, "A Metric and Frameworks for Resilience Analysis of Engineered and Infrastructure Systems," *Reliability Engineering & System Safety* 121 (2014): 91, https://doi.org/10.1016/j.ress.2013.07.004.

11 Alexandre Calado, Luís Capucha, and Kazimiera Maria Wódz, "Labour Relations under Duress in Europe: Contributions for Social Resilience Theory," *Sociologia – Problemas e Práticas*, no. 103 (2023): 11.

12 Ibid.

operate.[13] Furthermore, contemporary resilience research increasingly challenges individualistic and heroic framings of resilience, instead foregrounding collective, institutional, and policy dimensions that bear directly on labor law and workplace governance, as highlighted by Calado *et al.* and Dagdeviren *et al*. Empirical and conceptual studies in related fields further stress that fostering resilience in labor markets – and, by extension, in labor law contexts – requires addressing structural inequalities that shape workers' capacity to adapt to and recover from risks.[14] This involves interventions through organizational practices, supportive policies, and institutional or legal reforms. Such considerations align with emerging EU policy discussions on labor market resilience and social protection frameworks, particularly in the context of digitalization, labor market deregulation, and demographic change.[15] Such an integrated, critical resilience lens has significant implications for labor law and OSH governance, as it foregrounds the need for systemic reforms that enhance worker protection, equitable resource distribution, and institutional adaptability in the face of economic and technological changes.

Therefore, embedding psychosocial risk management within OSH law operationalizes resilience, both at the individual level – supporting workers' capacity to cope with stress and mental health-related factors – and at the structural level – strengthening organizational and legal systems to absorb and adapt to shocks, such as pandemics, digitalization, or rapid organizational change, thereby fostering sustainable and resilient organizational functioning. Unlike conventional occupational safety measures, which are largely prescriptive, this approach emphasizes anticipatory strategies, continuous monitoring, and systemic interventions to safeguard workers' mental health. In doing so, it bridges the standard organizational management perspective with the labor law approach, contributing to the "holistic, interdisciplinary framework" increasingly advocated in academic and policy discussions.

European legal frameworks, particularly the Framework Directive on Safety and Health at Work (89/391/EEC),[16] impose on employers a general duty to prevent "all risks" to the safety and health of workers, which has been interpreted to encompass psychosocial hazards and mental health risks in the workplace. Under Article 5 of this Directive, employers must ensure the safety and health of workers in all aspects of work, and the general principles of prevention – including risk assessment, risk elimination or reduction, and worker participation – apply to psychosocial hazards as well as physical ones. Complementing these binding obligations, EU soft law and social dialogue instruments – notably the European Framework Agreement on Work-Related Stress (2004)[17]

---

13 Hulya Dagdeviren et al., "Structural Foundations of Social Resilience," *Social Policy and Society* 19, no. 4 (2020): 539–52, https://doi.org/10.1017/S1474746420000032.

14 Rense Nieuwenhuis et al., "The Need and Capacity for Resilience in European Labor Markets: An Inequalities in Resilience Framework," rEUsilience Working Paper, Series 19, accessed January 11, 2026, https://osf.io/k8x2v_v2/.

15 Ibid.

16 Council Directive 89/391/EEC of 12 June 1989 on the Introduction of Measures to Encourage Improvements in the Safety and Health of Workers at Work (OJ L 183, 29 June 1989).

17 European Social Partners (ETUC, UNICE/BUSINESSEUROPE, UEAPME and CEEP), *Framework Agreement on Work-Related Stress*, October 8, 2004.

and the European Pact for Mental Health and Well-Being at Work (2008)[18] – provide non-binding guidance for the assessment, prevention, and management of psychosocial risks and work-related stress, reinforcing the normative expectation that psychosocial well-being is central to decent work, sustainable organizational governance, and institutional resilience.

While there is currently no dedicated EU "special directive" specifically on psychosocial risks, ongoing policy initiatives – including Commission communications on comprehensive approaches to mental health (2023) and peer reviews of legislative and enforcement practices in Member States – signal a continuing push at the EU level to strengthen protections for mental health and psychosocial risk prevention in OSH law and practice.[19]

The inclusion of "psychosocial risk in OSH law" thus integrates two domains: the legal domain, where enforceable obligations safeguard workers' mental health, and the organizational domain, where management practices, workplace culture, and structural design determine the realization of these protections. Normatively, integrating psychosocial risk management reflects the evolution of labor law toward safeguarding mental health as a core dimension of workplace rights. Practically, it equips organizations with mechanisms to identify, monitor, and mitigate risks that threaten workforce resilience and institutional functionality.[20] Within institutional and governance theory, the concept of resilience – which, as mentioned above, emphasizes a system's capacity to anticipate, absorb, adapt to, and recover from shocks while maintaining core functions and values[21] – implies, in the labor law context, that both legal frameworks and organizational structures must be equipped to safeguard workers' rights and protections amid uncertainty, crises, or rapid transformations. Thus, "institutional capacity" – encompassing regulatory standards, enforcement mechanisms, and organizational adaptability – becomes a critical determinant of whether labor rights, including psychosocial and mental well-being, are effectively safeguarded. By embedding resilience, i.e., psychosocial assessment and management, into governance, labor law moves beyond a reactive compliance model, fostering anticipatory mechanisms that simultaneously promote worker protection, organizational adaptability, and systemic stability. In doing so, it aligns the legal duty to protect with the normative goal of decent work. This approach is particularly important, given that empirical studies show conventional OSH regimes – historically focused on physical hazards – often overlook psychosocial dimensions, leaving both

18 European Commission, Directorate-General for Health and Food Safety, *European Pact for Mental Health and Well-Being*, adopted at the EU High-Level Conference "Together for Mental Health and Well-Being," Brussels, June 12–13, 2008.

19 European Commission, *Communication from the European Commission on a Comprehensive Approach to Mental Health and Psychosocial Risk Prevention in the EU* (Brussels, June 7, 2023).

20 Stephanie Duchek, "Organizational Resilience: A Capability-Based Conceptualization," *Business Research* 13, no. 1 (2020): 215–46, https://doi.org/10.1007/s40685-019-0085-7.

21 Małgorzata Pęciłło, "The Concept of Resilience in OSH Management: A Review of Approaches," *International Journal of Occupational Safety and Ergonomics* 22, no. 2 (2016): 291–300, https://doi.org/10.1080/10803548.2015.1126142.

workers and institutions vulnerable to stress-related disorders, burnout, and diminished organizational performance.[22]

From a broader normative and legal-theoretical standpoint, "embedding resilience within OSH law" reflects a shift from narrowly prescriptive rules toward principles-based governance, where the law not only mandates hazard prevention, but also cultivates the capacity of organizations and institutions to anticipate, absorb, and adapt to systemic disruptions. This approach positions psychosocial risk management as a central component of legal duties, reinforcing the normative expectation that employers and regulatory bodies safeguard workers' physical and mental integrity, even in conditions of uncertainty or crisis. Critically, "the resilience paradigm" exposes the limitations of traditional OSH regimes that focus on discrete, observable hazards, highlighting the need for legal frameworks capable of sustaining functional, rights-respecting workplaces through complex, socio-technical transformations, such as digitalization, pandemics, or economic shocks. In this sense, resilience is not merely an operational strategy, but a "normative principle" that integrates organizational adaptability, worker well-being, and systemic stability into the core purpose of labor law, thus advancing both decent work and social sustainability.

3. Serbia's Post-Pandemic OSH Legal Framework: Limits and Opportunities for Resilience

Serbia's OSH Act 2023[23] constitutes a significant legislative milestone, representing the first comprehensive reform of the national OSH framework in nearly two decades. Adopted by the National Assembly on April 28, 2023 – symbolically coinciding with the International Day for Safety and Health at Work – and promulgated in the Official Gazette of the Republic of Serbia No. 35/2023, the Act entered into force on May 7, 2023, formally replacing the long-standing 2005 OSH regime. The legislative impetus for this reform reflected profound transformations in work, including digitalization, the expansion of remote and home-based work, and the increasing flexibilization of employment relationships, as well as the need for closer alignment with European Union standards. These developments prompted the introduction of updated employer obligations, clearer regulation of non-standard work arrangements in relation to OSH protection, and a more explicit delineation of employers' responsibilities, including the duty to ensure occupational safety and health for employees working from home or remotely, in cooperation with employees, alongside revised conceptualizations of workplace safety. Nevertheless, despite signaling political commitment and regulatory modernization, the OSH Act 2023 remains limited in both normative depth and legal precision when assessed against contemporary international and European OSH standards.

Although the OSH Act 2023 strengthens procedural elements of risk assessment and introduces provisions on remote work and periodic medical examinations, it fails to incorporate psychosocial risk management and mental health protection as explicit, enforceable

[22] Agnieszka Krol et al. "Enhancing Workplace Safety: Addressing Psychosocial Hazards in Modern Organizations," *European Research Studies Journal* 28, no. 1 (2025): 696–706, https://doi.org/10.35808/ersj/3930.

[23] Serbia, *Occupational Safety and Health Act*, Official Gazette of the Republic of Serbia, No. 35/2023 (2023).

legal obligations. This omission constrains the resilience of Serbia's OSH system and reflects a broader continuity with conventional OSH regimes, which have historically prioritized physical hazards while marginalizing psychosocial risks. Such an approach persists, despite mounting evidence that psychosocial risks – stemming from inadequate work design, organizational practices, and adverse social relations at work – constitute major determinants of stress, anxiety, depression, burnout, and declining organizational performance.[24] The absence of a clear legal framework for psychosocial risk prevention thus represents a central deficiency of the new legislation. It underscores the need to reposition psychosocial risk management as a core component of Serbia's OSH regime.

Empirical and policy research consistently demonstrate that effective governance in this field requires clearly defined legal duties, including mandatory and continuous psychosocial risk assessments, structured methodologies, the involvement of social partners, and organizational measures aimed at preventing harm and promoting worker well-being, in line with EU and international best practices, particularly in the post-pandemic period.[25] As an example of good policy practice, the Spanish experience illustrates how the pandemic served as a catalyst for strengthening mental health governance within OSH frameworks. The COVID-19 pandemic in Spain was associated with a marked increase in mental health-related temporary work disabilities during the strict lockdown in 2020, generating substantial economic costs and exposing persistent gender disparities and sector-specific risks in relapse rates and absence durations.[26] Although both incidence and associated costs declined in 2021–2022, women continued to experience higher relapse rates and longer periods of work absence, underscoring the enduring mental health impact of the pandemic on workers.[27] In response, the crisis catalyzed a transformative policy shift, reviving the long-neglected national mental health strategy framework and leading to the adoption of the Spanish Strategy for Safety and Health at Work 2023–2027, which combined significant public investment with targeted, workplace-oriented measures. The Strategy emphasizes the equal protection of workers' physical and mental health. It sets out strategic objectives aimed at strengthening safeguards for vulnerable workers, including those with health vulnerabilities, integrating a gender-sensitive approach into OSH standards, and, notably, reinforcing the national OSH system to ensure effective preparedness and response to future crises.[28] According to the 2025 Report on Mental Health at Work in Spain, work-related psychological distress is conceptualized as a continuum ranging from normal, non-pathological suffering to mental health problems, such as burnout and clinically diagnosable mental disorders, underscoring

24 European Agency for Safety and Health at Work (EU-OSHA), "Strategies and Legislation on Psychosocial Risks in Six European Countries: Policy Brief."

25 Ibid.

26 Eva María Gutiérrez Naharro et al., "The Economic and Occupational Impact of Mental Health-Related Temporary Work Disabilities in Spanish Workers During and After the COVID-19 Pandemic: A Longitudinal Study," *Healthcare (Basel)* 13, no. 6 (2025): 618, https://doi.org/10.3390/healthcare13060618.

27 Ibid.

28 "The Spanish Strategy for Safety and Health at Work 2023–2027 Has Been Approved," International Labor Organization, 2023, accessed January 13, 2026, https://www.ilo.org/resource/news/spanish-strategy-safety-and-health-work-2023-2027-has-been-approved.

that not all work-related suffering should be medicalized or addressed primarily within the healthcare system. The 2025 Report emphasizes that effective protection of workers' mental health requires a "mental health in all policies" approach, prioritizing structural improvements in working conditions and coordinated preventive action across labor, social, and health systems, rather than an overreliance on individual diagnosis and pharmacological treatment.[29]

On the other hand, the Serbian OSH Act 2023 formally adheres to a proactive, preventive regulatory paradigm, consistent with prevailing trends in international, European, and comparative law. It establishes a comprehensive framework for preventing occupational injuries, occupational diseases, and work-related illnesses, while delineating the rights and obligations of employers and workers, and emphasizing information, consultation, cooperation, and training. However, notwithstanding this preventive orientation, the statutory text entirely omits any explicit reference to "psychosocial risks at work or to specific threats to mental health" arising from the interaction between work organization, social relations, and individual worker characteristics. Nor does it address the cumulative impact of organizational and social factors on mental and, consequently, physical health and overall workplace well-being. This normative silence reveals a structural limitation of the Act. It suggests that the legislator has not fully internalized the regulatory significance of emerging occupational risks shaped by technological change, organizational restructuring, and evolving social dynamics in the world of work, nor has it embraced the globally recognized (mental) "Health in All Policies" agenda.

Article 13 of the Serbian OSH Act 2023 defines the principles of prevention and, in paragraph 7, provides for the "development of a coherent prevention policy covering technology, work organization, working conditions, social relationships in the work process, and the influence of factors related to the working environment." This provision is a verbatim transposition of the relevant clause of Directive 89/391/EEC. While a purposive interpretation of this principle could lead to it being construed as encompassing psychosocial risks and other emerging occupational mental health hazards – mirroring the interpretative approach adopted at the EU level – the absence of explicit legal recognition significantly weakens its practical effectiveness.[30] Given that psychosocial risks remain insufficiently institutionalized, even in many advanced labor law systems, it is realistic to expect that, without further normative concretization, this provision will remain largely inoperative. For this reason, effective implementation would require regulatory "support" through secondary legislation, notably the adoption of a dedicated by-law specifically addressing psychosocial risks at work.[31]

Such a regulatory instrument should, at a minimum, provide a clear and legally precise definition of psychosocial risks and/or explicitly address specific psychosocial risks,

[29] "Trabajo y salud mental: hoja de ruta para las administraciones sanitarias en Espana," Ministerio De Sanidad Espana, 2025, accessed January 14, 2026, https://www.sanidad.gob.es/gabinetePrensa/notaPrensa/pdf/Hoja_250625184030855.pdf.

[30] Sanja Zlatanović and Andjelija Stevanović, "Upravljanje psihosocijalnim rizicima i izazovi zaštite mentalnog zdravlja u savremenom radnom pravu," *Radno i socijalno pravo: časopis za teoriju i praksu radnog i socijalnog prava* 27, no. 1 (2023): 227–49.

[31] Ibid.

encompassing a broader spectrum of work-related psychosocial hazards beyond the traditionally regulated categories of harassment and workplace violence, which in Serbia are governed by separate, specialized legislation. In addition, it should explicitly incorporate a holistic approach, aligned with the "Health in All Policies" framework, with specific reference to mental health protection. In this regard, valuable guidance can be drawn from comparative legal frameworks. In addition to the above-mentioned Spanish example, the Belgian legal framework, as articulated in the Well-Being at Work Code, explicitly defines specific psychosocial hazards – including work-related stress, burnout, harassment, and workplace violence – within a proactive, collective, and preventive conceptualization of psychosocial risks that places strong emphasis on organizational responsibility;[32] Furthermore, Swedish legislation, notably the Work Environment Act, originally enacted in 1977, adopts a holistic and integrative approach that closely links organizational conditions, work organization, and worker well-being, with particular emphasis on mental health, even though it does not provide an explicit statutory definition of psychosocial risks as such;[33] and French law has, since 2010, contained a general list of occupational risks, yet it has not explicitly identified psychosocial risks as a distinct regulatory category.[34] Nevertheless, subsequent legislative developments have progressively strengthened the prevention of work-related mental health risks. In particular, Law No. 2021–1018 reinforced the prevention of occupational mental health harms by emphasizing employers' responsibility for controlling workloads, especially in the context of telework.[35] When combined with the statutory right to disconnect introduced in 2017, these measures broaden the proactive and preventive approach to mental health at work in France, extending beyond individualized risk responses towards organizational and structural regulation of working conditions. These comparative models demonstrate how psychosocial risk regulation can be systematically integrated into OSH frameworks, enhancing proactive and preventive capacities, while strengthening legal certainty by explicitly including mental health protection within traditionally physical-risk-oriented OSH systems, thereby contributing to greater systemic resilience holistically.

The seriousness of this normative gap in the Serbian OSH Act 2023 is further underscored by comparative empirical evidence. Despite persistent shortcomings, the majority of EU Member States have, to varying degrees, explicitly addressed psychosocial risks and their implications for mental health within their general OSH legislation. In particular, factors such as excessive working time, shift and night work, workplace discrimination and harassment, and permanent digital availability have been legally recognized as occupational health risks. A comparative study conducted between December 2017 and February 2018 revealed that 82.3% of EU Member States and 16.6% of developed non-EU countries include provisions targeting specific psychosocial risks within their

[32] Aude Cefaliello, "Psychosocial Risks in Europe – National Examples as Inspiration for a Future Directive," ETUI Policy Brief, 2021, accessed January 18, 2026, https://www.etui.org/sites/default/files/2021-12/Psychosocial%20risks%20in%20Europe_2021_1.pdf.

[33] Ibid.

[34] Jean-Paul Dautel, "Psychosocial Risks in France," accessed December 23, 2025, https://www.etui.org/sites/default/files/2022-02/P3_JP_Dautel_PSR_in_France_2022_0.pdf.

[35] Ibid.

general OSH legislation. In contrast, among developing non-EU countries, only Albania and North Macedonia directly regulate psychosocial risks through OSH law.[36] Against this backdrop, the Serbian legislator's failure to address psychosocial risks and mental health protection clearly and systematically appears particularly difficult to justify.

From a legal-theoretical perspective, this omission also undermines the "normative resilience" of Serbia's OSH system. Regulatory resilience presupposes the capacity of legal frameworks to anticipate emerging risks, adapt to structural changes in work organization, and recover from systemic disruptions while maintaining core protective functions. By neglecting psychosocial risks – arguably among the most significant contemporary occupational hazards – the 2023 OSH Act limits its own ability to function as a resilient and future-oriented regulatory instrument. In an era characterized by digitalization, flexible work arrangements, and recurrent crises, the failure to integrate psychosocial risk governance and mental health protection represents not merely a technical legislative gap, but a structural weakness in the normative architecture of labor protection.

To enhance resilience, the Serbian legislator should explicitly integrate psychosocial risk management, requiring employers to undertake systematic risk assessments, define assessment frequency and methodology, and involve relevant stakeholders and social partners, thus ensuring proactive identification and mitigation of hazards that threaten both worker wellbeing and organizational continuity.[37] Mental health should be formally recognized within the scope of OSH law, with employers having obligations to prevent, monitor, and support employees through counseling, employee assistance programs, and organizational interventions, while providing adequate training for both managers and workers.[38] The inclusion of adaptive governance mechanisms – such as procedures for engaging social partners, task reallocation in crises, and safeguards for continuity of rights – would institutionalize resilience, enabling anticipation, absorption, and recovery from systemic disruptions.

Given the rapid expansion of remote and digitally mediated work, OSH obligations should extend beyond physical ergonomics to encompass psychological and organizational dimensions, ensuring that remote work environments are governed in line with holistic occupational safety and resilience principles. Strengthening labor inspection capacity to monitor compliance with psychosocial requirements, accompanied by specialized training for OSH practitioners and transparent reporting systems, would help translate aspirational resilience principles into enforceable legal practice. Without such reform, the Serbian OSH 2023 Act's omissions regarding psychosocial risk management, mental health protection, and adaptive labor governance will continue to limit its capacity to function as a resilient, future-proof legal system capable of protecting workers and preserving institutional integrity in an increasingly unpredictable world.

---

36 Zlatanović and Stevanović, "Upravljanje psihosocijalnim rizicima i izazovi zaštite mentalnog zdravlja u savremenom radnom pravu."

37 International Labor Organization and World Health Organization, "Mental Health at Work: Policy Brief."

38 "Mental Health at Work," World Health Organization, accessed December 6, 2025, https://www.who.int/news-room/fact-sheets/detail/mental-health-at-work.

4. Conclusion

This study demonstrates that the COVID-19 pandemic exposed significant structural vulnerabilities in Serbia's labor law system, particularly its capacity to safeguard OSH and ensure the continuity of workers' rights during public health emergencies. Applying the lens of resilience theory, the findings reveal that Serbia's post-pandemic OSH reforms, including the 2023 OSH Act, have not sufficiently enhanced the system's adaptive, absorptive, or transformative capacities. While temporary measures during the pandemic addressed immediate needs, the absence of integrated mental health protections, psychosocial risk management, and formal mechanisms for emergency labor regulation indicates that the system remains largely reactive rather than resilient.

From a resilience perspective, strengthening the labor law framework requires a shift from a traditional, physically oriented OSH approach to one that incorporates psychosocial well-being, preventive stress management, and structured support for workers during crises. Building normative resilience entails not only codifying emergency measures and flexible work arrangements, but also fostering institutional capacities for social dialogue, enforcement, and adaptive governance. Such reforms are essential to ensure that Serbia's labor system can absorb shocks, maintain continuity of workers' rights, and adapt effectively to future disruptions.

Funding: This paper was written as part of the 2026 Research Program of the Institute of Social Sciences supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia.

References

Calado, Alexandre, Luís Capucha, and Kazimiera Maria Wódz. "Labour Relations under Duress in Europe: Contributions for Social Resilience Theory." *Sociologia – Problemas e Práticas*, no. 103 (2023): 9–29. https://doi.org/10.7458/SPP202310328458.

Cefaliello, Aude. "Psychosocial Risks in Europe: National Examples as Inspiration for a Future Directive." ETUI Policy Brief, 2021. Accessed January 18, 2026. https://www.etui.org/sites/default/files/202112/Psychosocial%20risks%20in%20Europe_2021_1.pdf.

Dagdeviren Hulya, Luis Capucha, Alexandre Calado, Matthew Donoghue, and Pedro Estêvão. "Structural Foundations of Social Resilience." *Social Policy and Society* 19, no. 4 (2020): 539–52. https://doi.org/10.1017/S1474746420000032.

Dautel, Jean-Paul. "Psychosocial Risks in France." Accessed December 23, 2025. https://www.etui.org/sites/default/files/202202/P3_JP_Dautel_PSR_in_France_2022_0.pdf.

Duchek, Stephanie. "Organizational Resilience: A Capability-Based Conceptualization." *Business Research* 13, no. 1 (2020): 215–46. https://doi.org/10.1007/S40685-019-0085-7.

Duffy, Ryan D., Haram J. Kim, Nicholas P. Gensmer, Trisha L. Raque-Bogdan, Richard P. Douglass, Jessica W. England, and Aysenur Buyukgoze-Kavas. "Linking Decent Work with Physical and Mental Health: A Psychology of Working Perspective." *Journal of Vocational Behavior* 112 (2019): 384–95. https://doi.org/10.1016/j.jvb.2019.05.002.

Eurofound and EU-OSHA. *Psychosocial Risks in Europe: Prevalence and Strategies for Prevention*. Luxembourg: Publications Office of the European Union, 2014.

European Agency for Safety and Health at Work (EU-OSHA). "Strategies and Legislation on Psychosocial Risks in Six European Countries: Policy Brief," 2025. Accessed January 8, 2026. https://osha.europa.eu/en/publications/strategies-and-legislation-psychosocial-risks-six-european-countries.

European Commission. *Communication from the European Commission on a Comprehensive Approach to Mental Health and Psychosocial Risk Prevention in the EU*. Brussels, June 7, 2023.

European Commission. Directorate-General for Health and Food Safety. *European Pact for Mental Health and Well-Being*. Adopted at the EU High-Level Conference "Together for Mental Health and Well-Being," Brussels, June 12–13, 2008.

European Foundation for the Improvement of Living and Working Conditions (Eurofound). "Psychosocial Risks." Accessed December 5, 2025. https://www.eurofound.europa.eu/en/topics/psychosocial-risks.

European Social Partners (ETUC, UNICE/BUSINESSEUROPE, UEAPME and CEEP). *Framework Agreement on Work-Related Stress*. October 8, 2004.

Francis, Royce, and Behailu Bekera. "A Metric and Frameworks for Resilience Analysis of Engineered and Infrastructure Systems." *Reliability Engineering & System Safety* 121 (2014): 90–103. https://doi.org/10.1016/j.ress.2013.07.004.

Gutiérrez Naharro, Eva María, José Antonio Ponce Blandón, Amalia Sillero Sillero, and José Fernández Sáez. "The Economic and Occupational Impact of Mental Health-Related Temporary Work Disabilities in Spanish Workers During and After the COVID-19 Pandemic: A Longitudinal Study." *Healthcare (Basel)* 13, no. 6 (2025): 618. https://doi.org/10.3390/healthcare13060618.

International Labor Organization and World Health Organization. "Mental Health at Work: Policy Brief." Accessed December 10, 2025. https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40ed_protect/%40protrav/%40safework/documents/publication/wcms_856976.pdf.

International Labor Organization. "The Spanish Strategy for Safety and Health at Work 2023–2027 Has Been Approved," 2022. Accessed January 13, 2026. https://www.ilo.org/resource/news/spanish-strategy-safety-and-health-work-2023-2027-has-been-approved.

Krol, Agnieszka, Jolanta Żygadło, Katarzyna Ochyra-Żurawska, Aneta Chrząszcz, Julia Nowicka. "Enhancing Workplace Safety: Addressing Psychosocial Hazards in Modern Organizations." *European Research Studies Journal* 28, no. 1 (2025): 696–706. https://doi.org/10.35808/ersj/3930.

Leka, Stavroula, and Tom Cox, eds. *The European Framework for Psychosocial Risk management (PRIMA-EF)*. Nottingham: Institute of Work, Health and Organization, 2008.

Lerouge, Loïc. "The Concepts of 'Mental Health in the Workplace' and 'Psychosocial Risks': A Clarification from a Legal Perspective." *European Labour Law Journal* 16, no. 3 (2025): 377–83. https://doi.org/10.1177/20319525251336018.

Ministerio De Sanidad Espana. "Trabajo y salud mental: hoja de ruta para las administraciones sanitarias en Espana." Accessed January 14, 2026. https://www.sanidad.gob.es/gabinetePrensa/notaPrensa/pdf/Hoja_250625184030855.pdf.

Nieuwenhuis, Rense, Max Thaning, Alzbeta Bartova, and Lovisa Backman. "The Need and Capacity for Resilience in European Labor Markets: An Inequalities in Resilience Framework." rEUsilience Working Paper Series 19. Accessed January 11, 2026. https://osf.io/k8x2v_v2/.

Pęciłło, Małgorzata. "The Concept of Resilience in OSH Management: A Review of Approaches." *International Journal of Occupational Safety and Ergonomics* 22, no. 2 (2016): 291–300. https://doi.org/10.1080/10803548.2015.1126142.

Rossi, Maria Francesca, Maria Rosaria Gualano, Nicola Magnavita, Umberto Moscato, Paolo Emilio Santoro, and Ivan Borrelli. "Coping with Burnout and the Impact of the COVID-19 Pandemic on Workers' Mental Health: A Systematic Review." *Frontiers in Psychiatry* 14, 1139260 (2023). https://doi.org/10.3389/fpsyt.2023.1139260.

Şahin, Didem Rodoplu, Mustafa Aslan, Harun Demirkaya, and Hülya Ateşoğlu. "The Effect of COVID-19 on Employees' Mental Health." *Scientific Reports* 12, 15067, (2022). https://doi.org/10.1038/s41598-022-18692-w.

Schulte, Paul A., Steven L. Sauter, Sudha P. Pandalai, Hope M. Tiesman, Lewis C. Chosewood, Thomas R. Cunningham, Steven J. Wurzelbacher et al. "An Urgent Call to Address Work-Related Psychosocial Hazards and Improve Worker Well-Being." *American Journal of Industrial Medicine* 67, no. 6 (2024): 499–514. https://doi.org/10.1002/ajim.23583.

World Health Organization. "Mental Health at Work." Accessed December 6, 2025. https://www.who.int/news-room/fact-sheets/detail/mental-health-at-work.

Zlatanović, Sanja, and Stevanović Anđelija. "Upravljanje psihosocijalnim rizicima i izazovi zaštite mentalnog zdravlja u savremenom radnom pravu." *Radno i socijalno pravo: časopis za teoriju i praksu radnog i socijalnog prava* 27, no. 1 (2023): 227–49.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 169–193
https://doi.org/10.31743/recl.19828
Received: 16 February 2026 | Accepted: 6 March 2026 | Published: 31 March 2026

Volatility as a Legal Challenge: Rethinking Labor Law Responses to Workplace Violence – European Approach

Łucja Kobroń-Gąsiorowska

PhD habil., Assistant Professor, Institute of Law, Economics and Administration, University of the National Education Commission, Krakow; correspondence address: ul. Podchorążych 2, 30–084 Kraków, Poland; e-mail: l.kobron@nckg.pl
https://orcid.org/0000-0002-8669-452X

Abstract: Workplace violence is a growing concern in contemporary labor law, driven by its prevalence and volatile nature. Effective legal analysis requires understanding volatility as the variability, unpredictability, repetition, and context-dependence of violent and abusive conduct. Workplace violence is not isolated or uniform but is shaped by changing social, economic, organizational, and regulatory factors. Its forms, intensity, frequency, and visibility shift over time, across sectors, and among different groups, especially regarding gender and socio-economic status. This volatility exposes the limitations of uniform regulatory models that assume stable risks. Evidence from Europe and Central Asia shows that violence and harassment are often recurrent, disproportionately affect women, and persist despite strong legal frameworks. The frequent occurrence of psychological and sexual harassment, along with underreporting in precarious or low-income settings, highlights gaps between formal legal protections and their practical effectiveness. Volatility impacts not only the occurrence of violence but also access to remedies, reporting, enforcement, and employer compliance. The protective function of labor law depends on its ability to address these volatile patterns. Volatility challenges complaint-based models and underscores the need for preventive, ongoing, and context-sensitive legal duties. This includes gender-sensitive risk assessments, differentiated employer obligations, and recognition of repeated violence as an aggravated violation, as well as greater attention to psychosocial harm. By viewing workplace violence as an evolving risk, the author advocates for a new approach to labor regulation in Europe that prioritizes substantive equality, early intervention, and effective enforcement over formally neutral but insufficient standards.

Keywords: volatility, workplace violence, harassment, psychosocial risks, risk assessment

1. Introduction

Violence in the workplace has become a significant challenge for contemporary labor law, reflecting broader changes in employment relations and workplace organization. "Workplace violence" encompasses a range of unacceptable behaviors, including physical violence, verbal abuse, threats, bullying, psychological harassment, and sexual harassment. These behaviors can cause physical, psychological, sexual, or economic harm to individuals.[1] Previously, workplace violence was viewed mainly as an occupational health or interpersonal issue, but it is now increasingly recognized as a legal problem

[1] International Labour Organization, *Violence and Harassment Convention, 2019 (No. 190)*, accessed January 10, 2026, https://www.ilo.org/dyn/normlex/en/f?p=normlexpub:12100:0::no::p12100_ilo_code:r206.

ISSN 2545-384X (Online)

requiring systemic regulatory responses.[2] From a labor law perspective, workplace violence raises fundamental questions concerning the protection of human dignity, equality, and the right to safe and healthy working conditions. In accordance with international legal standards, the most notable of which is the International Labour Organization's Violence and Harassment Convention, 2019 (No. 190)[3] establishes a broad framework that obliges states to prevent, prohibit, and remedy such conduct across all sectors. This reflects a consensus that labor law must address both physical and psychosocial risks in modern workplaces. Research shows that workplace violence has serious and lasting effects on workers' mental and physical health, including increased risks of anxiety, depression, burnout, and post-traumatic stress disorder. These harms also lead to broader social and economic costs, such as reduced productivity, higher absenteeism, and increased turnover, reinforcing the need for effective legal regulation.[4] Labor law is critical in defining employer responsibilities, enforcement mechanisms, and access to remedies for affected workers. This article analyzes key variables that determine violence in labor law, including legal definitions and conceptualization. The author argues that violence in labor law is a broad concept, and any behavior intended to cause physical or psychological harm in the workplace is relevant. Such behavior creates a pathological situation that employers must address or minimize.

The volatility of workplace violence is characterized by heterogeneity, manifested in its variability and unpredictability.[5] The form, intensity, frequency, perpetrators, and groups affected vary depending on the social, economic, organizational, and political context. It is imperative to acknowledge this diversity to formulate effective labor policies and regulations. Primarily, this necessitates establishing regulations that can proactively prevent the emergence of various manifestations of workplace violence. The primary objective of the research question presented is to conceptualize workplace violence as a heterogeneous, context-dependent phenomenon rather than a single, uniform issue. The objective of the present study is to move beyond conventional, simplistic definitions by underscoring heterogeneity across multiple dimensions. Future researchers of workplace violence should set four objectives: identify and categorize forms of workplace violence by examining differences in form, intensity, frequency, types of perpetrators, and groups affected by violence. The following analysis should be carried out: an examination of the contextual conditions, social, economic, organizational, and political factors that shape how workplace violence arises and manifests itself in different environments. The impact of this variability on existing labor policies and regulatory frameworks should

2 Valerio De Stefano et al., "Platform Work and the Employment Relationship" (ILO Working Paper 2021), 133–62, https://econpapers.repec.org/paper/iloilowps/995121493302676.htm.

3 International Labour Organization, *Violence and Harassment Convention*.

4 International Labour Organization, *Recommendation Concerning the Elimination of Violence and Harassment in the World of Work (No. 206)* (2019), accessed March 10, 2026, https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:R206; World Health Organization, *Guidelines on Mental Health at Work* (Geneva: WHO, 2022), https://www.who.int/publications/i/item/9789240053052.

5 See also: Jiwook Jung, Zoltán Lippenyi, and Eunmi Mun, "Workplace Volatility and Gender Inequality: A Comparison of the Netherlands and South Korea," *Socio-Economic Review* 20, no. 4 (2022): 1679–740, https://doi.org/10.1093/ser/mwab026.

be assessed, with particular attention to cases where a one-size-fits-all approach is insufficient. Evidence-based policy development should be grounded in a nuanced understanding to support the design of targeted, flexible, and context-specific labor regulations.

This article aims to understand workplace violence as a dynamic, volatile phenomenon rather than a constant or uniform issue from a European[6] perspective. Interrelated factors, including social elements such as gender relations, migration status, and power imbalances, shape the forms, intensity, frequency, and visibility of workplace violence. Economic conditions, such as labor market insecurity, unemployment, and sectoral competition, also contribute, as do organizational factors, including hierarchies, management practices, employment contracts, and workplace culture. The political and regulatory context, including labor law frameworks and enforcement mechanisms, is also crucial in shaping workplace violence. Given the complexity of the issue, this article focuses on selected variables and literature. The analysis uses the latest statistics from the International Labour Organization (ILO), while recognizing that further research is needed to address the outlined objectives fully.

2. Violence at Work? And Why Do We Care?

In contrast to the analytical approach adopted by Celia M. Geck *et al.*, in the article "Violence at Work,"[7] a thorough examination of aggressive, violent, and repeatedly violent employees reveals that the decision to investigate workplace aggression and workplace violence as separate constructs is not sufficiently supported on theoretical or empirical grounds. The authors of the study argue for a categorical distinction between these behaviors. However, existing literature in the fields of occupational psychology and forensic psychiatry increasingly conceptualizes aggression and violence as points along a single behavioral continuum.[8] This is differentiated mainly by severity and immediate consequences rather than by distinct etiological processes. The approach taken in their study, which treats aggression and violence as discrete phenomena, risks fragmenting the analysis of shared risk factors and obscuring pathways to escalation. It is important to note that persistent, low-level aggression may ultimately culminate in overt violence. Consequently, the separation employed by Geck *et al.* may limit the explanatory scope of their findings and reduce the study's utility for developing comprehensive workplace prevention and intervention strategies. The fundamental argument of this article, and one that is of particular significance from the perspective of labor law, is the observation that the aforementioned distinction is irrelevant to labor law. Within the domain of labor law, the act itself is significant, as dysfunctional behavior engenders pathology in the workplace. Within the domain of labor law, the act itself is significant, as dysfunctional behavior

6 And several countries in Central Asia.

7 Carter M. Geck et al., "Violence at Work: An Examination of Aggressive, Violent, and Repeatedly Violent Employees," *Journal of Threat Assessment and Management* 4, no. 4 (2017): 210–29, https://doi.org/10.1037/tam0000091.

8 Sharon M. Boles and Karen Miotto, "Substance Abuse and Violence: A Review of the Literature," *Aggression and Violent Behavior: A Review Journal* 8, no. 2 (2003): 155–74, http://dx.doi.org/10.1016/S1359-1789(01)00057-X.

engenders pathology in the workplace. Workplace safety is frequently called into question when highly visible and severe incidents, such as workplace homicides or mass killings, dominate media coverage. However, it should be noted that nonphysical forms of aggression, including harassment and bullying, occur far more frequently than acts of physical violence, including assaults and homicides. Nevertheless, both direct exposure to and witnessing of such behaviors have been demonstrated to be associated with substantial adverse outcomes. The consequences of such incidents can be manifold, including heightened fear of future violent incidents, reduced employee morale and job performance, and negative effects on workers' physical, emotional, and psychological well-being.[9] There has been substantial progress in the theoretical and empirical examination of aggressive and violent behavior in the workplace. A significant proportion of this progress has been dedicated to identifying and analyzing risk factors associated with aggressive behavior in a broader context.[10]

I have to admit that significant advances have been made in theoretical and empirical domains, providing a solid foundation for understanding workplace aggression. However, addressing the ongoing conceptual challenges, particularly the distinction between aggression and violence, remains a pivotal area for future research.[11] In accordance with this perspective, a number of scholars contend that workplace aggression and violence should be regarded as distinct conceptual phenomena, necessitating their separate examination. This standpoint asserts that an analysis of aggressive and violent behavior in the workplace is imperative. A significant proportion of this progress has

[9] Nathan A. Bowling and Terry A. Beehr, "Workplace Harassment from the Victim's Perspective: A Theoretical Model and Meta-Analysis," *Journal of Applied Psychology* 91, no. 5 (2006): 998–1012, http://dx.doi.org/10.1037/0021-9010.91.5.998; Robert A. Baron and Joel H. Neuman, "Workplace Aggression – The Iceberg beneath the Tip of Workplace Violence: Evidence on Its Forms, Frequency, and Targets," *Public Administration Quarterly* 21, no. 4 (1998): 446, https://www.jstor.org/stable/40861725.

[10] Bowling and Beehr, "Workplace Harassment from the Victim's Perspective"; James Bonta and D.A. Andrews, "Risk-Need-Responsivity Model for Offender Assessment and Rehabilitation," *Rehabilitation*, no. 6 (2007): 1–22.

[11] Lynne M. Andersson and Christine M. Pearson, "Tit for Tat? The Spiralling Effect of Incivility in the Workplace," *Academy of Management Review* 24, no. 3 (1999): 452–71, https://doi.org/10.5465/amr.1999.2202131; Baron and Neuman, "Workplace Aggression," 446–62; Bowling and Beehr, "Workplace Harassment from the Victim's Perspective"; Ståle V. Einarsen et al., eds., *Bullying and Harassment in the Workplace: Developments in Theory, Research, and Practice*, 2nd ed. (Boca Raton: CRC Press, 2011); M. Sandy Hershcovis and Julian Barling, "Towards a Multi-Foci Approach to Workplace Aggression: A Meta-Analytic Review of Outcomes from Different Perpetrators," *Journal of Organizational Behavior* 31, no. 1 (2010): 24–44, https://doi.org/10.1002/job.621; Loraleigh Keashly and Karen Jagatic, "North American Perspectives on Hostile Behaviors and Bullying at Work," in *Bullying and Harassment in the Workplace*, eds. Ståle Einarsen et al. (Boca Raton: CRC Press, 2011), 41–71; Paul Linsley, *Violence and Aggression in the Workplace* (Boca Raton: CRC Press, 2018); Joel H. Neuman and Robert A. Baron, "Aggression in the Workplace: A Social-Psychological Perspective," in *Counterproductive Work Behavior: Investigations of Actors and Targets*, eds. Suzy Fox and Paul E. Spector (Washington: American Psychological Association, 2005), 13–40; Paul E. Spector and Suzy Fox, "The Stressor–Emotion Model of Counterproductive Work Behavior," in *Counterproductive Work Behavior: Investigations of Actors and Targets*, eds. Suzy Fox and Paul E. Spector (Washington: American Psychological Association, 2005), 151–74; Dieter Zapf and Ståle Einarsen, "Bullying in the Workplace: Recent Trends in Research and Practice – An Introduction," *European Journal of Work and Organizational Psychology* 10, no. 4 (2001): 369–73, https://doi.org/10.1080/13594320143000807; M. Sandy Hershcovis et al., "Predicting Workplace Aggression: A Meta-Analysis," *Journal of Applied Psychology* 92, no. 1 (2007): 228–38, https://doi.org/10.1037/0021-9010.92.1.228.

been dedicated to identifying and analyzing risk factors associated with aggressive behavior in a broader context.[12]

Therefore, this paper treats workplace aggression and workplace violence as a single concept, which does not, however, preclude the identification of many forms of violence not covered in this article due to the multifaceted nature of violence. For linguistic systematization only, I will distinguish between them, although, as I emphasize, violence can be aggression in labor law. The term "workplace aggression" is defined as intentional behavior by an employee that is directed towards harming another employee or results in such harm, with primary emphasis on psychological rather than physical injury.[13] Examples of such behaviors include verbal abuse, intimidation, humiliation, bullying, harassment, and deliberate property damage. In contrast, the term "workplace violence" refers to behaviors that result in or are intended to result in physical harm to another employee. Such behaviors may include physical assault, attempted assault, unwanted sexual contact, or confrontations involving weapons or improvised instruments. Although instances of workplace violence are not particularly prevalent, the most extreme manifestations of such behavior include workplace homicides and mass murder events. The latter are defined as incidents in which at least four employees are killed during a single episode.[14]

The categorization of workplace aggression and violence is a complex undertaking, and it is imperative to recognize the significance of the relationship between the perpetrator and the victim when conducting such analyses. Offenders in category I possess no legitimate relationship to the organization or its employees. They enter the workplace with the intent to commit a crime, such as robbery or theft. Workplace homicides frequently fall into this category. Type II occurs when the perpetrator, typically a client or student, has a legitimate relationship with the organization and engages in aggression or violence during service interactions. It has been determined that approximately 60% of workplace aggression incidents are classified as Type II. Type III refers to incidents in which both the perpetrator and the victim are current or former employees. The following factors may contribute to the occurrence of such incidents: individual characteristics (e.g., personality traits or prior aggression); organizational factors (e.g., perceived injustice); and supervisory practices. Type IV encompasses perpetrators who are not affiliated with the organization, yet have previously maintained, or continue to maintain, a close personal relationship with an employee.[15]

The most recent approach, proposed by Paul Linsley, highlights that one of the main challenges in addressing violence and aggression is the difficulty of clearly defining them.[16] The concepts of violence and aggression are subjective in nature and are interpreted differently by different individuals and groups. Consequently, the impact of

12 Bonta and Andrews, "Risk-Need-Responsivity Model."

13 Aaron C.H. Schat and E. Kevin Kelloway, "Workplace Aggression," in *Handbook of Work Stress*, eds. Julian Barling, E. Kevin Kelloway, and Michael R. Frone (Thousand Oaks: Sage, 2005), 189–218.

14 James Alan Fox and Jack Levin, *Extreme Killing: Understanding Serial and Mass Murder*, 3rd ed. (Thousand Oaks: Sage, 2014).

15 Julian Barling, Kathryne E. Dupré, and E. Kevin Kelloway, "Predicting Workplace Aggression and Violence," *Annual Review of Psychology* 60 (2009): 671–92, https://doi.org/10.1146/annurev.psych.60.110707.163629.

16 Paul Linsley dismisses medical workers (Linsley, *Violence and Aggression in the Workplace*).

violence varies depending on the individual's experience. Consequently, healthcare organizations and professional groups have developed multiple definitions of violence and aggression, each serving a distinct purpose. Nevertheless, for healthcare personnel to competently identify, respond to, and prevent violence and aggression, they must possess a clear and thorough understanding of these concepts. This necessitates a description that encompasses the manifold forms of violence and aggression, while still allowing room for personal interpretation and understanding. This approach has been shown to engender a sense of responsibility among staff members regarding the issue at hand, thereby offering a modicum of validation of their concerns.

In addressing this issue, Paul Linsley employs a range of established institutional definitions to conceptualize workplace violence and aggression.[17] In particular, he cites the definition proposed by the Department of Health, which characterizes violence and aggression as any work-related incident in which staff are abused, threatened, intimidated, or assaulted, thereby posing either an explicit or implicit risk to their safety, well-being, or health. Paul Linsley observes that this understanding closely aligns with the definition adopted by the Health Development Agency, which similarly defines such incidents as those in which individuals employed within the healthcare sector are insulted, threatened, or attacked by patients or members of the public in circumstances connected to their work.

Paul Linsley draws on these definitions to emphasize that workplace violence should not be narrowly understood as physical assault alone. It is important to note that the concept under discussion also encompasses non-physical behaviors. These include, but are not limited to, verbal abuse, gestures, and other conduct that may induce fear, a sense of threat, or humiliation in the recipient. Threats may be perceived or actual, and physical injury is not a necessary criterion for an incident to constitute violence within the workplace. Furthermore, Linsley refers to the broader conceptualization offered by the International Labour Organization, which defines workplace violence as any form of behavior that results in harmful physical or emotional consequences for workers in the course of their employment. It is important to note that this definition acknowledges the potential for unintentional harm. Such harm could be attributed to factors such as cultural differences or individual preferences regarding interpersonal interaction and treatment in professional contexts.[18] Additionally, Linsley alludes to the definition promulgated by the Counter Fraud and Security Management Service, a specialist body within the National Health Service that wields overarching responsibility for the management of violence and aggression in healthcare contexts. This definition is narrow in scope, delineating violence as the deliberate application of force against another individual without lawful justification, thereby resulting in physical injury or personal discomfort. However, Linsley notes that such a definition excludes unintentional violence, for instance, that arising from a patient's cognitive impairment following head trauma sustained in a road traffic accident. Linsley's position is that, irrespective of the definition ultimately adopted, it must be meaningful to those who apply it in practice and enable clear recognition of the problem.

17 Based in the UK.

18 International Labour Organization, *Violence and Harassment Convention*.

Furthermore, he contends that the promotion of awareness of violence and aggression within healthcare environments is at least as important as the definition of these phenomena. He also emphasizes that, irrespective of definitional boundaries, violence and aggression in professional life may manifest in a wide variety of forms, necessitating consideration and examination of the diverse ways in which such behaviors can occur. In conclusion, a singular descriptive definition is put forward, as per which, as P. Linsley contends, aggressive or violent behavior may be comprehended as encompassing: uncivil conduct, distinguished by an absence of respect for others; physical or verbal aggression, entailing an intention to inflict harm; and assault, delineated as the deliberate intent to injure another person. He proposes a classification system in which aggression is characterized as a combination of physical or verbal, active or passive, and direct or indirect forms:

> A. Physical, active, direct aggression includes isolated, acute incidents that typically involve physical violence, such as a drunken fight, an assault, or an attack by a confused patient, as well as routine or chronic acts like ongoing physical or sexual abuse or bullying;
>
> I. The following typology of aggression has been proposed:
>
> II. Physical, active, indirect aggression: the persuading of another person to inflict harm, for example, by endorsing physical punishment as a disciplinary method.
>
> III. Physical, passive, direct aggression: the physical prevention of someone from achieving a desired goal, such as when a senior colleague deliberately blocks access to a workstation.
>
> IV. Physical, passive, indirect aggression: the refusal to carry out necessary tasks.
>
> V. Verbal, active, direct aggression: the insulting or humiliating of another person, such as through name-calling or racial or sexual slurs.
>
> VI. Verbal, active, indirect aggression: the spreading of malicious rumors or the undermining of others' self-confidence by belittling their abilities or appearance.
>
> VII. Verbal, passive, direct aggression: the refusal to speak or respond to questions.
>
> VIII. Verbal, passive, indirect aggression: the avoidance of responsibility for expressing one's views, for instance, by failing to defend someone who is being unfairly criticized.[19]

Within this theoretical framework, aggression can be defined as any behavior intentionally directed at causing harm or injury to another individual. However, as previously mentioned, aggressive acts may also be unintentional. Nevertheless, as previously mentioned, aggressive acts may also be unintentional. Furthermore, aggression may be directed either externally, towards others, or internally, towards oneself, as evidenced by instances of self-harm. Property damage constitutes a form of violence, albeit one that does not directly threaten the safety of staff. Nevertheless, it can be distressing and unsettling for witnesses. Consequently, aggression should be understood as a continuum of behaviors ranging from verbal or emotional acts to severe physical injury. It is imperative to acknowledge that manifestations of aggression can be expressed in written form, via email or telephone. This renders such behaviors more accessible to staff than ever before.[20]

---

19 Based on research by Arnold H. Buss, *The Psychology of Aggression* (New York: Wiley, 1961).

20 Linsley, *Violence and Aggression in the Workplace*.

It is also crucial to emphasize that violence and aggression are inextricably linked, and, from a labor law perspective, any conceptual distinction between these terms is legally inconsequential. Labor law does not attribute normative consequences to the semantic distinction between "aggression" and "violence," treating both notions as functionally equivalent forms of conduct that infringe legally protected interests. From the perspective of labor law, the decisive element is the occurrence of violent behavior itself, irrespective of its classification or terminology, together with the volatility in which it arose. Legal relevance is therefore attributed primarily to the existence of violence within the employment relationship and to the causal and contextual factors underlying such conduct, rather than to theoretical or definitional distinctions between aggression and violence.

3. Volatility and Why Does It Matter?

In common language, the term "volatility" is used to denote the degree to which a situation fluctuates or lacks stability. When applied to the context of violence in the workplace, this concept can be used to describe the changing intensity, frequency, or forms of harmful behavior experienced by employees over time. Behavior of this nature may manifest in a variety of forms, ranging from isolated incidents to recurring patterns of aggression, harassment, or intimidation. Such behavior has the potential to engender an unstable and unpredictable work environment.[21] From an analytical perspective relevant to labor law and occupational safety, this variability may concern a single aspect of workplace violence, such as the escalation or de-escalation of hostile conduct towards an employee, or the interaction between multiple factors, including power imbalance, organizational culture, workload, and management response. These elements may fluctuate in tandem, reinforcing one another, thereby shaping the overall risk profile faced by workers. Conventionally, the assessment of workplace violence is conducted over defined reference periods, such as reporting cycles, employment durations, or statutory monitoring intervals. However, it can also be meaningfully examined over very short timeframes, capturing immediate or momentary changes in behavior that may trigger legal duties to intervene. This approach is consistent with contemporary labor law frameworks that emphasize employers' ongoing responsibility to prevent, identify, and respond promptly to psychosocial risks in the workplace.

In this article, aggression and violence in the workplace are examined within the framework of employment law. The focus is on legally relevant factors for the identification, assessment, and prevention of prohibited conduct, including unlawful interpersonal violence in the workplace. As demonstrated in the International Labour Organization's *Experiences of Violence and Harassment at Work* survey in Europe and Central Asia, violence and harassment in the workplace persist as a substantial problem, impacting

[21] Torben G. Andersen and Tim Bollerslev, *Volatility* (Northampton: Edward Elgar, 2018), https://public.econ.duke.edu/~boller/Published_Papers/AB_Volatility_Introduction_18.pdf; Fabio Rumler and Johann Scharler, "Labor Market Institutions and Macroeconomic Volatility in a Panel of OECD Countries" (European Central Bank Working Paper No. 1005, 2008), https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1005.pdf.

25.5% of employed individuals throughout their professional careers.[22] This places the region among the highest-prevalence regions globally, second only to the Americas. A significant proportion of those affected reported that their most recent experience occurred within the five years preceding the survey, indicating that the problem is not only historical but ongoing. The magnitude of gender disparities in Europe and Central Asia is especially pronounced. The gender gap in terms of violence and harassment at work was found to be one of the most significant observed worldwide. Specifically, it was determined that women were 8.0 percentage points more likely than men to have experienced violence or harassment at work during their working lives. This finding indicates that workplace violence and harassment in the region affect women to a greater extent than in other global regions. The European data demonstrate that violence and harassment in the workplace are prevalent and entrenched issues, accompanied by a discernible gender imbalance, necessitating sustained policy focus and targeted preventive interventions.

For the purposes of this article, due to the limitations of the publication format, we will focus on three common and culturally neutral types of workplace violence. These are physical violence and harassment, such as hitting, restraining or spitting, psychological violence and harassment, such as insults, threats, bullying or intimidation, sexual harassment and violence, such as unwanted sexual touching, comments, pictures, emails or sexual requests.[23]

In Europe and Central Asia, 25.5% of respondents reported having personally experienced workplace violence or harassment at least once during their working lives. This figure exceeds the global average, thereby indicating a comparatively elevated incidence or disclosure rate within the region. From a regulatory standpoint, this prevalence indicates that workplace violence and harassment are not merely isolated incidents but rather part of a systemic occupational risk. The data demonstrate a marked gender disparity: women constitute 30.0% of the sample and men 22.0%. This discrepancy of approximately eight percentage points signifies a disproportionate impact on women, aligning with prevailing research findings on gender-based violence and harassment in employment settings. The persistence of this gap indicates that current legal safeguards and equality frameworks have not yet fully mitigated gender-specific exposure to harm. The predominance of recent incidents suggests that workplace violence and harassment in Europe and Central Asia are current and ongoing violations (18.3% of incidents within the past five years), rather than residual effects of past workplace norms. This temporal concentration raises concerns about the effectiveness of enforcement mechanisms, compliance oversight, and the preventive obligations imposed on employers. The data indicate that incidents of workplace violence and harassment in Europe and Central Asia persist at high levels, exhibiting gender-based differences and a contemporary pattern. The high incidence and recent occurrence of reported incidents indicate that existing legal and institutional frameworks, while robust in formal terms, require strengthened

22 *Experiences of Violence and Harassment at Work: A Global First Survey* (Geneva: International Labour Organization and Lloyd's Register Foundation, 2022), https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@dgreports/@dcomm/documents/publication/wcms_863095.pdf.

23 Ibid.

implementation, accountability mechanisms, and preventive obligations to ensure the effective protection of workers' dignity, safety, and fundamental rights.

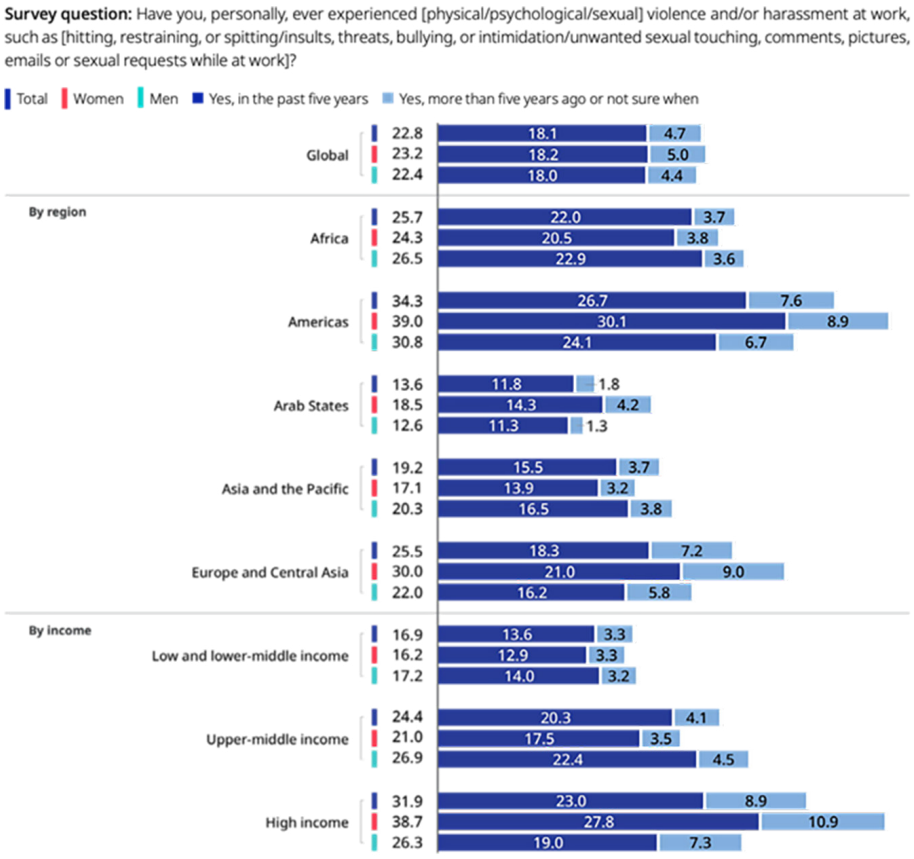

Fig. 1. (ILO, *Experiences of Violence and Harassment at Work: A Global First Survey* [Geneva: International Labour Organization and Lloyd's Register Foundation, 2022])

The data reveals a clear, income-based volatility in the prevalence of workplace violence and harassment. As national income levels increase, reported prevalence rises across all genders and time frames. This pattern suggests differential exposure, reporting capacity, and regulatory effectiveness across income groups. For instance, Low- and Lower-Middle-Income Economies (total prevalence: 16.9%, women: 16.2%, men: 17.2%) have the lowest reported prevalence in this income category, with minimal gender differentiation. While this could suggest a lower incidence, it more plausibly reflects underreporting, driven by weaker enforcement mechanisms, limited access to complaint procedures, precarious employment conditions, and fear of retaliation. The relatively low proportion of historical reports further supports the inference of structural barriers to disclosure.

4. Physical Violence and Harassment

It is evident that Europe and Central Asia demonstrate comparatively low incidences of reported workplace violence and harassment, exhibiting minimal gender disparity. The correlation between income level and prevalence is not straightforward; high-income countries do not necessarily have higher prevalence. It is hypothesized that reporting culture and legal awareness may inflate observed rates in high-income contexts, particularly for women. The persistence of non-zero rates across all groups underscores the conclusion that workplace violence and harassment are systemic, global issues, not confined to poorer regions.

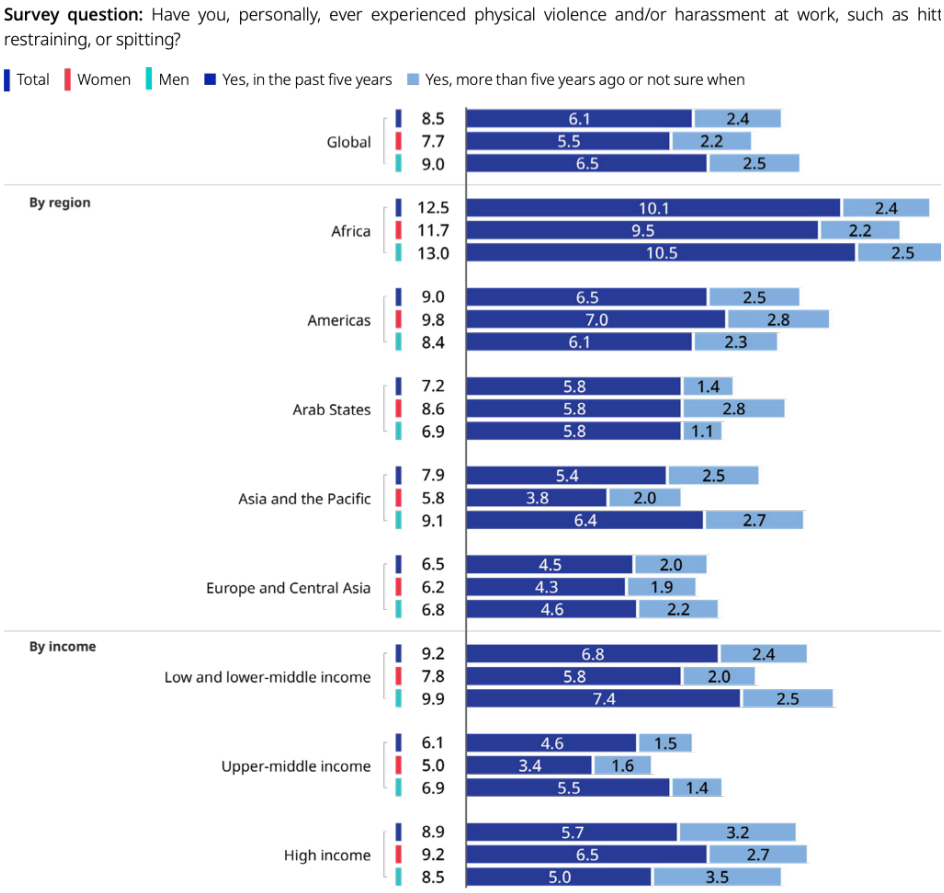

Fig. 2. (ILO, *Experiences of Violence and Harassment at Work*)

Europe and Central Asia report approximately 50% of the prevalence observed in Africa. In comparison with the Americas, Europe's rate is approximately 30% lower. This positions Europe as one of the lowest-risk regions globally in terms of reported workplace physical violence and harassment. European women report substantially lower exposure than women in both Africa and the Americas. The question, therefore, arises: why

does Europe achieve superior outcomes? This phenomenon can be attributed to a number of factors, including the implementation of more robust labor inspection regimes, higher levels of formal employment, clearer legal definitions accompanied by effective enforcement mechanisms, and well-established institutional procedures for addressing workplace grievances.

5. How Often?

A survey of respondents in Europe and Central Asia reveals that more than 48% of them report having experienced workplace violence or harassment on at least three occasions. This finding suggests that such incidents are frequently systemic or recurring rather than isolated events. In contrast, Europe and Central Asia are characterized by persistent exposure to violence, affecting both women and men. It has been reported that female subjects indicated experiencing harassment on a slightly more frequent basis (at least three times).

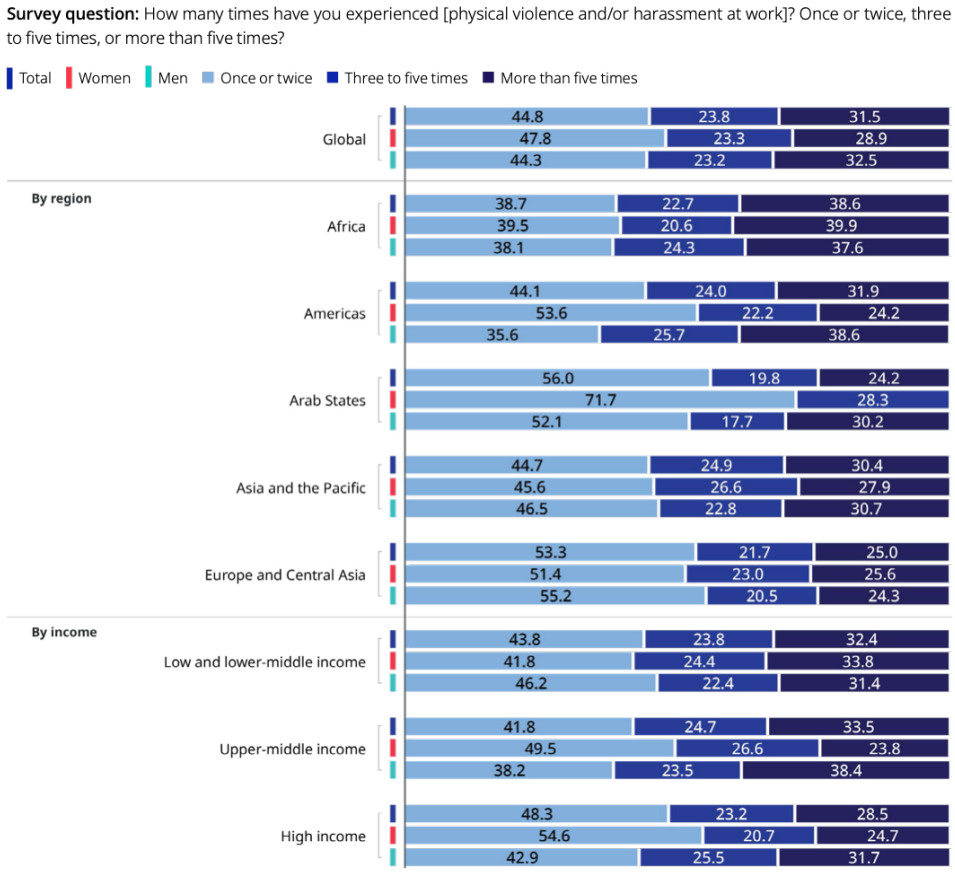

Fig. 3. (ILO, *Experiences of Violence and Harassment at Work*)

The male demographic is predominantly represented in the "once or twice" category. The observed disparity is less pronounced than that observed in regions such as the Arab States or the Americas. This observation may indicate the presence of more effective reporting mechanisms for both genders, or of more comparable exposure patterns across genders in European workplaces. Furthermore, Europe exhibits a lower incidence of single or rare incidents, yet a higher prevalence of repeated exposure, particularly within the "more than five times" category. This phenomenon can be attributed to organizational tolerance or ineffective enforcement, in which incidents of harassment are not addressed after initial occurrences, victims remain exposed for extended periods, and perpetrators face limited consequences. The data suggest that formal protections alone are insufficient without robust internal reporting, accountability mechanisms, and organizational-level cultural change.

6. Psychological Violence and Harassment at Work

In comparison with the global average, Europe and Central Asia demonstrate comparatively elevated levels of psychological violence and/or harassment. The combined prevalence for women and men in the region stands at 19.8%, exceeding the global mean of 17.9%. This indicates that psychological violence constitutes a significant and widespread problem rather than a marginal phenomenon.

This elevated prevalence positions the region at a global premium, underscoring the issue's significance from both social and policy perspectives. A marked gender disparity is evident in the data. The present study found that women reported experiencing psychological violence at a substantially higher rate (22.7%) than men (17.4%), resulting in a gender gap of approximately 5.3 percentage points. This finding is one of the largest observed across all regions and indicates that women in Europe and Central Asia encounter psychological violence with greater frequency than men. However, this discrepancy may also be due to a higher level of awareness, recognition, and willingness to report such experiences among the female population. It is noteworthy that this gender gap is considerably larger than those observed in Africa or the Asia-Pacific region and is broadly comparable to patterns seen in the Americas. The temporal dimension of the data further underscores the urgency of the problem. A considerable proportion of the documented cases transpired within the preceding half-decade, signifying that psychological violence is not merely a matter of historical legacy but a present and continuous concern. It has been reported that women, in particular, have higher levels of recent exposure than men, thus serving to reinforce concerns about the existence of persistent gendered risks in contemporary work and social environments. Compared with Europe and Central Asia, prevalence levels in the Americas are higher than those observed in Africa, the Asia-Pacific region, and the Arab States, but lower than those in Europe and Central Asia. The regional pattern closely aligns with those observed in upper-middle and high-income countries, suggesting that economic development and higher income levels do not, in themselves, eliminate the risk of psychological violence. A salient nuance pertains to the socio-economic context of reporting.

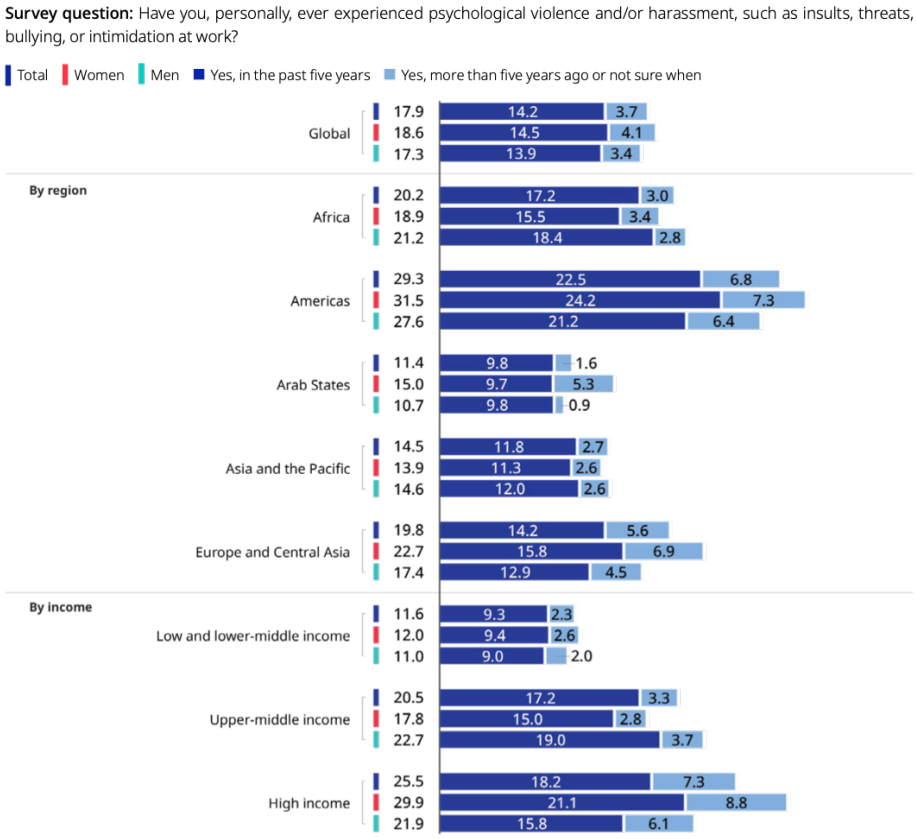

Fig. 4. (ILO, *Experiences of Violence and Harassment at Work*)

The fundamental issue is that Europe and Central Asia exhibit considerable overlap with higher-income groups, which have been shown, globally, to report at higher rates. This may be indicative of a heightened awareness of psychological violence, a reduction in stigma associated with disclosure, and an enhancement in the recognition of non-physical forms of abuse within survey instruments. Nevertheless, it is important to note that increased reporting levels do not necessarily lead to a diminution in the perceived severity of the problem. Instead, they serve to underscore the persistent prevalence of psychological violence, even within more economically developed contexts. The evidence indicates that psychological violence in Europe and Central Asia is more prevalent than the global average, disproportionately affects women, and frequently occurs in the recent past. The findings demonstrate that economic development alone is insufficient as a protective factor and point to the need for gender-sensitive, contemporary prevention strategies and policy interventions.

7. How Many Times? How Often?

Europe and Central Asia demonstrate a distinct pattern in the frequency of reported experiences, one that is driven less by isolated incidents and more by repeated exposure. In this region, 36.9% of respondents report experiencing the issue once or twice, 21.0% report it three to five times, and 42.1% report more than five occurrences. This distribution is proximate to the global mean in the lowest frequency category (36.8% globally), but it diverges distinctly in the higher frequencies.

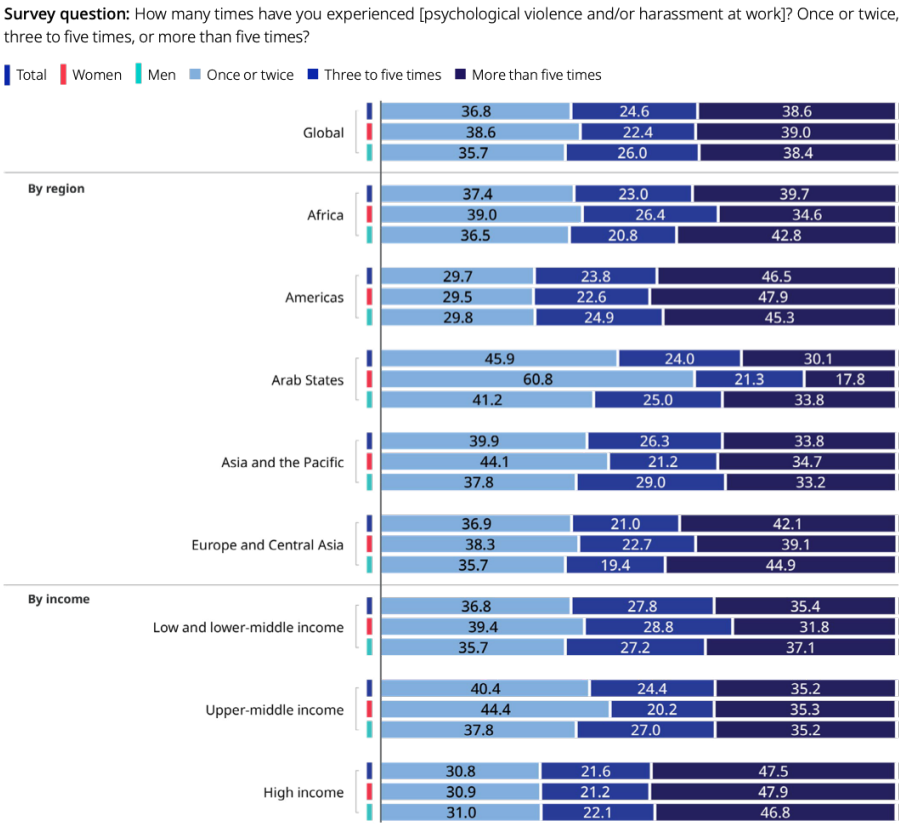

Fig. 5. (ILO, *Experiences of Violence and Harassment at Work*)

Europe has a smaller share of mid-frequency cases (24.6% globally versus 21.0% in Europe) and a larger share of high-frequency cases (38.6% globally versus 42.1% in Europe). In percentage-point terms, Europe is essentially identical to the global level for one-off incidents; however, a shift away from the "3–5 times" category is evident, indicating a tendency towards chronic or recurrent exposure. In other words, Europe's higher figures are not driven by more people experiencing a single incident, but by more people experiencing repeated incidents. This pattern is reinforced by

Europe's position in the regional comparison for the most severe frequency category. With 42.1% of respondents reporting more than five occurrences, Europe and Central Asia rank second-highest among all regions, behind the Americas (46.5%) and ahead of Africa (39.7%), Asia and the Pacific (33.8%), and the Arab States (30.1%). This places Europe near the top globally in terms of persistent, repeated experiences rather than sporadic ones.

The evidence presented here suggests that gender differences within Europe and Central Asia further refine this picture. Amongst female respondents, 38.3% report experiencing the issue once or twice, 22.7% report three to five instances, and 39.1% report more than five instances. For men, the corresponding figures are 35.7%, 19.4%, and 44.9%. A comparison of the data reveals that, unlike women, men are under-represented in the lower- and mid-frequency categories and over-represented in the highest category. The proportion of men reporting more than five occurrences is 5.8 percentage points higher than that of women.

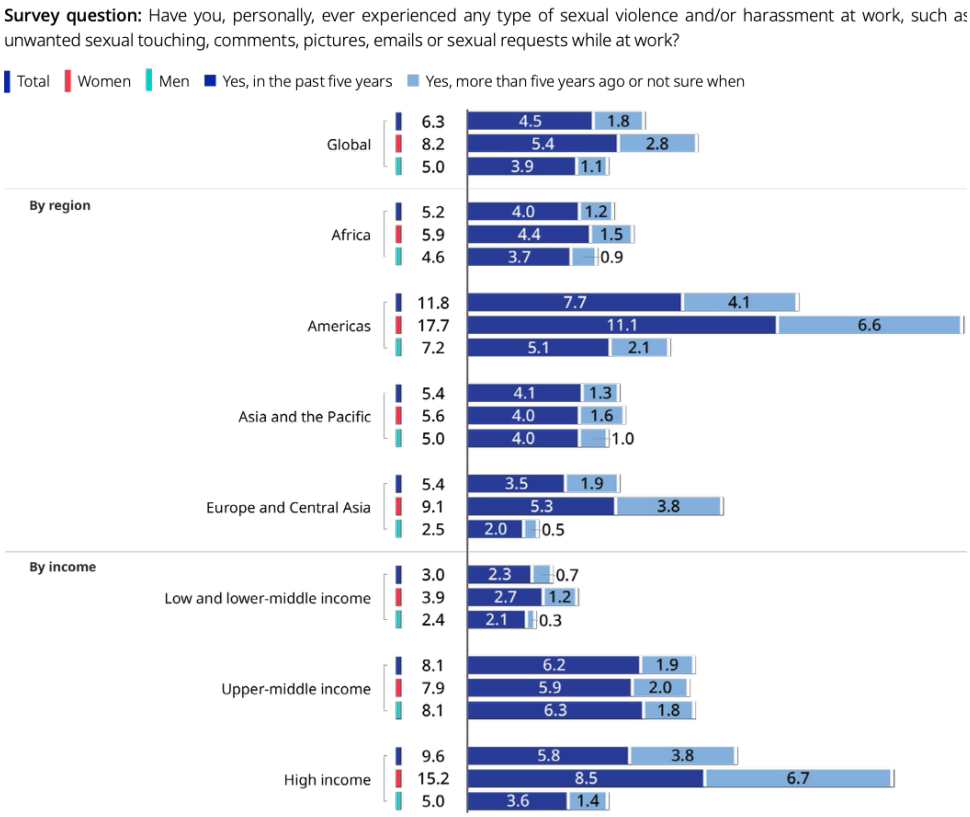

Fig. 6. (ILO, *Experiences of Violence and Harassment at Work*)

This finding indicates that, among individuals who report experiencing harassment in Europe and Central Asia, males are more inclined to categorize the harassment

as highly repetitive. At the same time, females are comparatively more concentrated in the lower-frequency categories. When considered as a whole, the distribution suggests a degree of polarization within Europe. The proportion of one-off incidents closely mirrors the global average, yet the proportion of very frequent incidents is higher, and the mid-range category is smaller. This pattern is consistent with situations that, once they occur, are more likely to persist rather than remain limited. When interpreted in terms of workplace risk, Europe's profile appears less as a series of isolated incidents and more as a series of ongoing situations, such as repeated exposure, unresolved conflicts, or repeat perpetrators within specific teams or roles.

The findings of this paper indicate that Europe and Central Asia exhibit a prevalence of sexual violence and harassment at work that is closely aligned with the global average. This observation suggests that such issues are not anomalous occurrences in the region but rather reflect broader societal challenges. However, the frequency distribution indicates that persistence and repetition remain a significant concern, thereby emphasizing the gravity of the issue rather than diminishing it.

8. Gender Differences

The gender disparity in experiences of sexual violence and harassment in the workplace is particularly evident in Europe and Central Asia. The prevalence of workplace sexual harassment and violence against women is a matter of concern, with approximately 9.1% of women reporting such experiences, in contrast to the approximately 2.5% of men who have experienced similar incidents. This indicates that women are reporting such experiences at a rate more than three times that of men. This disparity is among the widest observed globally and is comparable to the gender gap in the Americas. The data indicates that workplace sexual misconduct in Europe disproportionately affects women, despite the region's generally stronger legal and institutional frameworks. When compared with other regions, Europe and Central Asia display a mixed profile. The overall prevalence rates are lower than those observed in the Americas, especially in women, but are broadly similar to those observed in the Asia-Pacific region. Nevertheless, Europe is distinguished by its pronounced gender divide. Concurrently, a higher prevalence of such behavior has been reported among European men compared to their African counterparts. This discrepancy may be indicative of heightened awareness of the definition of harassment, reduced stigma around reporting such incidents, and more extensive or inclusive conceptualizations of workplace misconduct. It is hypothesized that several structural factors shape these patterns. A heightened propensity to disclose may also be a contributing factor, as enhanced labor protections, institutional mechanisms, and social norms can promote disclosure, particularly among female respondents. Concurrently, entrenched power imbalances within the workplace perpetuate gender disparities, despite explicit commitments to gender equality. Hierarchical structures continue to render women susceptible to elevated levels of risk. Furthermore, the category "Europe and Central Asia" comprises a highly diverse set of countries, suggesting that national prevalence rates likely vary considerably beneath the regional average. The findings indicate that instances of sexual violence and harassment in the European

and Central Asian workplace are not as infrequent as might be presumed. It is estimated that approximately one in eleven women has experienced this phenomenon directly, thereby highlighting the magnitude of the problem. The analysis indicates that gender inequality emerges as the predominant driver, superseding considerations of overall economic development or institutional capacity. While legal frameworks are relatively robust, they are insufficient in isolation. To be effective, robust enforcement mechanisms, meaningful organizational culture change, and effective prevention measures must accompany them.

In conclusion, Europe and Central Asia present a clear paradox: moderate overall prevalence combined with strong gender polarization. This finding suggests that, while general workplace standards may be comparatively high, women continue to bear a disproportionate burden of sexual harassment and violence at work. It is, therefore, imperative that targeted, gender-specific interventions be implemented to address this issue, rather than broad, generic policy approaches. Sexual violence or harassment at work.

9. How Often? How Many Times?

Approximately 50% of respondents in Europe and Central Asia report having been subjected to sexual violence and/or harassment at work on more than one occasion. The most prevalent response was "once or twice," with "more than five times" ranking second. This suggests that repeated exposure is pervasive rather than exceptional. When broken down by gender, women report the highest prevalence across all frequency categories. It is evident that a considerable proportion of women have indicated that they have experienced the phenomenon on multiple occasions, with a significant number reporting three to five instances or more, suggesting chronic exposure rather than isolated incidents. Men report a lower overall prevalence, and their experiences are more heavily concentrated in the "once or twice" category. This suggests that when incidents occur, they tend not to be repeated. The pattern for the total population closely mirrors that of women, reflecting women's heavier weighting in reported cases. In comparison with other regions, Europe and Central Asia largely follow the global pattern in which women consistently report higher frequency and repetition than men, and repeated harassment (three or more times) is a substantial issue rather than an outlier. Concurrently, there are significant regional variations.

Compared with regions such as Africa and Asia, and the Pacific, Europe and Central Asia show a marginally higher proportion of experiences reported to occur "more than five times" and a concomitant reduction in the prevalence of incidents reported only once. This finding suggests the presence of systemic or ongoing workplace issues rather than sporadic events.

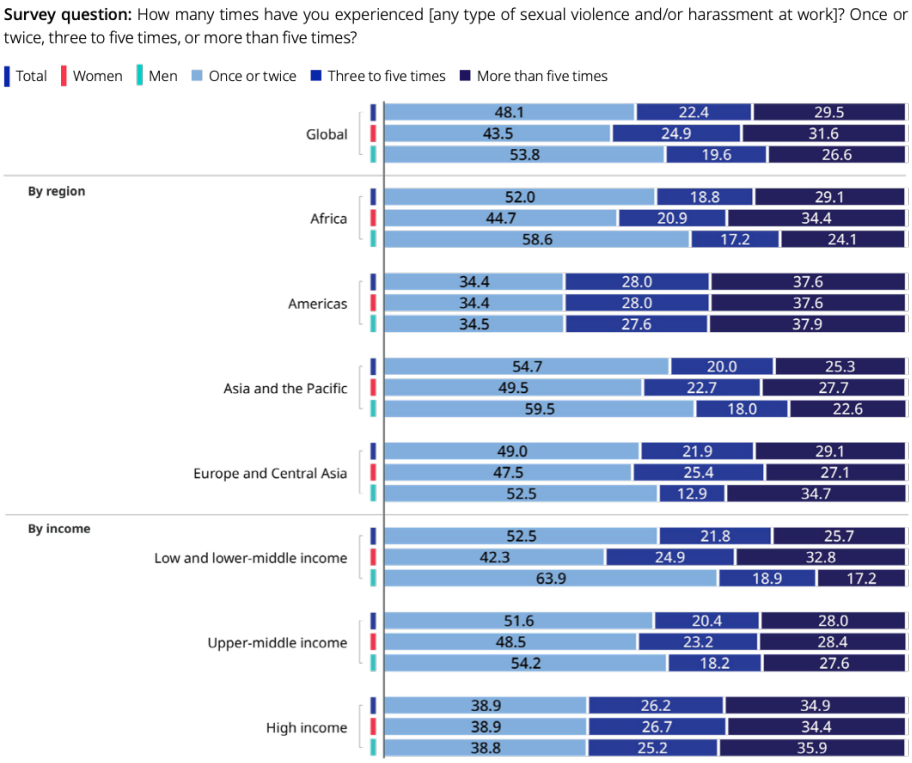

Fig. 7. (ILO, *Experiences of Violence and Harassment at Work*)

When evaluated in its entirety, the data indicate that, in Europe and Central Asia, occurrences of sexual harassment and violence in the workplace are more prevalent as a recurring phenomenon rather than as isolated incidents. The markedly elevated incidence of reporting by women, notably with regard to repeated experiences, underscores gendered power imbalances and the potential inadequacies of prevention and reporting mechanisms. Despite relatively robust legal frameworks in many European countries, the recurrence of incidents suggests deficiencies in enforcement, workplace culture, or the effectiveness of internal reporting systems. The key conclusion is that sexual violence and harassment in the workplace in Europe and Central Asia are widespread, frequently recurring, and disproportionately affecting women. This finding suggests that these issues are not merely the result of isolated misconduct but rather reflect entrenched workplace dynamics. Consequently, more robust prevention measures, enhanced accountability frameworks, and organizational follow-through mechanisms that extend beyond formal policies are imperative.

10. Volatilities and Their Impact on Protection against Violence in the Workplace

The empirical data presented in the analyzed material reveal several legally significant volatilities in the occurrence, reporting, and persistence of workplace violence and harassment, which directly affect the effectiveness of the protection afforded under labor law. It is evident from the evidence presented that workplace violence cannot be regarded as a uniform or incidental risk. Rather, it should be considered a structurally differentiated phenomenon, which highlights the limitations of formally robust legal frameworks when confronted with unequal social and institutional conditions.[24]

Firstly, a marked gender-based volatility is evident across all forms of workplace violence and harassment that have been examined. It has been reported that women consistently indicate a higher lifetime prevalence of exposure, as well as a greater repetition of harmful conduct, particularly within specific categories. This discrepancy is especially pronounced in cases of sexual violence and harassment, where women report experiencing these behaviors at a rate that is more than three times higher than men. From a labor law perspective, this volatility underscores the inadequacy of formally gender-neutral protective norms. While general duties to safeguard dignity, health, and safety apply equally to all workers, the neutral formulation of these duties fails to account for gendered power asymmetries inherent in many employment relationships. Consequently, extant legal protections do not operate with equal effectiveness in practice. This necessitates the incorporation of gender-sensitive preventive duties, differentiated risk assessment obligations, and enhanced procedural safeguards to ensure substantive equality.[25]

Secondly, the data reveal a marked, income-based volatility in reported prevalence, with lower rates observed in low- and lower-middle-income economies and higher rates recorded in upper-middle- and high-income contexts. This variation cannot be interpreted as reflecting actual differences in incidence alone. Instead, it highlights variations in reporting capacity, legal awareness, institutional accessibility, and enforcement effectiveness. In lower-income settings, structural barriers such as insecure employment, limited labor inspection, and fear of retaliation significantly constrain the exercise of legal rights. Consequently, the protection afforded by labor law against violence in these contexts is often formal rather than effective, underscoring the reliance on institutional capacity and procedural accessibility rather than on legislative norms alone.

A further legally relevant dimension of workplace violence concerns its temporal dimension. The concentration of reported incidents within the past five years indicates that violence and harassment are not merely residual phenomena associated with outdated workplace norms, but rather ongoing violations of workers' rights. This temporal

[24] See also: Louise F. Fitzgerald and Lilia M. Cortina, "Sexual Harassment in Work Organizations: A View from the 21st Century," in *APA Handbook of the Psychology of Women*, eds. Cheryl B. Travis et al., vol. 2, *Perspectives on Women's Private and Public Lives* (American Psychological Association, 2018), 215–34, https://doi.org/10.1037/0000060-012; Einarsen et al., eds., *Bullying and Harassment in the Workplace*, 3–24, 87–110, 381–98.

[25] Vincent J. Roscigno, "Social Movement Struggle and Race, Gender, Class Inequality," *Race, Sex & Class* 2, no. 1 (1994): 109–26, https://www.jstor.org/stable/41680099; Dieter Zapf and Ståle Einarsen, "Mobbing at Work: Escalated Conflicts in Organisations," in *Counterproductive Work Behavior: Investigations of Actors and Targets*, eds. Suzy Fox and Paul E. Spector (Washington: American Psychological Association, 2005), 575–99.

volatility raises significant concerns about the adequacy of enforcement mechanisms and employer compliance with preventive obligations. From a regulatory standpoint, it is suggested that ex post remedies based on individual complaints are insufficient, and that labor law should place greater emphasis on continuous preventive duties, monitoring requirements, and employer accountability for failing to intervene at an early stage. A close association with this temporal aspect is evident in the volatility of frequency, which is characterized by a high proportion of workers reporting repeated and chronic exposure rather than isolated incidents. The preponderance of harassment, defined as instances of victimization that have occurred at least three times, and frequently more than five times, signifies organizational tolerance or a systemic failure to rectify misconduct once it has come to light. From a legal standpoint, this phenomenon highlights a fundamental weakness in the enforcement of labor laws. The absence of effective escalation mechanisms enables the perpetration of harmful conduct despite formal prohibitions. The ongoing exposure workers face has a detrimental effect on the protective function of labor law. This exposure necessitates the recognition of repeated violence and harassment as aggravated violations, thereby triggering heightened employer liability.

Finally, the data reveal that different forms of violence exhibit varying degrees of volatility, with psychological violence emerging as particularly prevalent despite being less visible and more challenging to substantiate than physical violence. This disparity highlights an imbalance in labor law, which has traditionally prioritized physical safety while providing weaker and more ambiguous protection against psychological harm. The high prevalence and persistence of psychological harassment highlight the need for clearer legal definitions and evidentiary adaptations, as well as proactive employer duties that address non-physical forms of abuse. Taken together, these volatilities reveal that the effectiveness of labor law protection against workplace violence depends not only on the existence of formal legal norms, but also on their ability to address differentiated risks, power imbalances and institutional constraints. Without addressing gendered exposure, socio-economic disparities, temporal persistence and the repetitive nature of harm, labor law risks offering nominal rather than substantive protection. Effective regulation, therefore, requires a shift from abstract, uniform standards towards differentiated, preventive and enforcement-oriented approaches, capable of ensuring the real and equal protection of workers' dignity, safety and fundamental rights.

11. Conclusions

Despite the extensive empirical material presented, the analysis is deficient from a labor law perspective because it fails to incorporate several legally and normatively indispensable variables for assessing the effectiveness of protection against workplace violence and harassment. Omitting these variables significantly limits the ability to draw well-founded conclusions regarding risk allocation, regulatory sufficiency, and the scope of employer obligations.

Firstly, the lack of systematic disaggregation by economic sector and occupational category represents a substantial analytical shortcoming. From a labor law perspective, exposure to violence and harassment varies significantly across sectors and professions.

Heightened risks tend to prevail in contexts involving intensive interpersonal interaction, structural subordination, or sustained engagement with third parties. Examples of such contexts include healthcare, education, social services, hospitality, and security. Without sector-specific differentiation, it is impossible to ascertain whether the legal duties imposed on employers accurately reflect the varying risk profiles or whether heightened, sector-specific preventive obligations are necessary. This omission undermines the assessment of the proportionality and suitability of regulatory measures. Secondly, the analysis does not sufficiently consider employment status and contractual form, including the distinction between open-ended and fixed-term contracts, temporary agency work, platform-mediated labor, informal employment and economically dependent self-employment. This omission is of direct legal relevance, as workers in non-standard or precarious employment relationships frequently experience diminished levels of effective protection and face structural barriers to reporting misconduct. They are also more vulnerable to retaliatory practices. A comprehensive evaluation of labor-law protection against workplace violence must consider the accessibility and enforceability of safeguards across different contractual arrangements. Thirdly, the absence of variables relating to organizational size and workplace structure limits the scope of the legal analysis. The existence and effectiveness of internal compliance mechanisms, reporting procedures, and preventive policies vary substantially between large enterprises and small or micro-employers. Without disaggregated data by organizational size, it is impossible to assess the realizability of statutory duties, particularly those concerning prevention, internal procedures, and monitoring, across different categories of employers, or whether differentiated regulatory techniques are warranted. Fourthly, the analysis does not consider variables relating to migrant status, ethnicity, disability, age, or other intersecting grounds of vulnerability. From a contemporary labor and equality law perspective, this omission is particularly consequential. Violence and harassment often occur at the intersection of multiple vulnerability factors, so failing to capture these dimensions risks concealing compounded and systemic forms of harm. Without such data, legal responses will remain insufficiently targeted and may fail to meet the requirements of substantive equality and non-discrimination. Fifthly, insufficient attention is paid to workplace power relations, including hierarchical position, managerial authority, and dependency linked to performance evaluation or job security.

Whether the offender is a supervisor, co-worker, or third party, such as a client or customer, has substantial legal implications, particularly regarding employer liability, preventive obligations, and the allocation of responsibility. Without this information, it is difficult to assess whether existing legal frameworks adequately address vertical violence and abuses of authority, which are key concerns in modern labor law. Furthermore, a critical deficiency is the lack of data on the availability, accessibility, and effectiveness of internal and external complaint mechanisms. While the material provides information on prevalence and frequency, it does not systematically address reporting behavior, employer responses, or the provision of remedies. From a legal standpoint, protection against violence and harassment is inseparable from procedural effectiveness. Without information on reporting pathways, outcomes, and protection against retaliation, it is impossible to evaluate whether labor law guarantees meet the fundamental right

to an effective remedy. Finally, the analysis omits variables relating to legal awareness and training among both workers and employers. Awareness of rights, understanding of prohibited conduct and knowledge of available remedies can greatly influence reporting practices and preventive compliance. Without this dimension, it is impossible to distinguish between high prevalence resulting from increased exposure to risk and that resulting from greater legal literacy and awareness, which is essential for evaluating regulatory effectiveness.

In conclusion, although the existing data provide valuable insights into the prevalence, gender differences, and persistence of workplace violence and harassment, the omission of variables relating to sectoral context, employment status, organizational structure, intersectional vulnerability, workplace power relations, complaint mechanisms, and legal awareness substantially limits labor law analysis. Without these elements, evaluating the efficacy, accessibility, and enforceability of labor-law protection in practice remains an abstract concept.

References

Andersen, Torben G., and Tim Bollerslev. *Volatility*. Northampton: Edward Elgar, 2018. https://public.econ.duke.edu/~boller/Published_Papers/AB_Volatility_Introduction_18.pdf.

Andersson, Lynne M., and Christine M. Pearson. "Tit for Tat? The Spiraling Effect of Incivility in the Workplace." *Academy of Management Review* 24, no. 3 (1999): 452–71. https://doi.org/10.5465/amr.1999.2202131.

Barling, Julian, Kathryne E. Dupré, and E. Kevin Kelloway. "Predicting Workplace Aggression and Violence." *Annual Review of Psychology* 60 (2009): 671–92. https://doi.org/10.1146/annurev.psych.60.110707.163629.

Baron, Robert A., and Joel H. Neuman. "Workplace Aggression – The Iceberg beneath the Tip of Workplace Violence: Evidence on Its Forms, Frequency, and Targets." *Public Administration Quarterly* 21, no. 4 (1998): 446–64. https://www.jstor.org/stable/40861725.

Boles, Sharon M., and Karen Miotto. "Substance Abuse and Violence: A Review of the Literature." *Aggression and Violent Behavior* 8, no. 2 (2003): 155–74. https://doi.org/10.1016/S1359-1789(01)00057-X.

Bonta, James, and D.A. Andrews. "Risk-Need-Responsivity Model for Offender Assessment and Rehabilitation." *Rehabilitation*, no. 6 (2007): 1–22.

Bowling, Nathan A., and Terry A. Beehr. "Workplace Harassment from the Victim's Perspective: A Theoretical Model and Meta-Analysis." *Journal of Applied Psychology* 91, no. 5 (2006): 998–1012. https://doi.org/10.1037/0021-9010.91.5.998.

Buss, Arnold H. *The Psychology of Aggression*. New York: Wiley, 1961.

De Stefano, Valerio, Ilda Durri, Charalampos Stylogiannis, and Mathias Wouters. "Platform Work and the Employment Relationship." ILO Working Paper 2021. https://econpapers.repec.org/paper/iloilowps/995121493302676.htm.

Einarsen, Ståle V., Helge Hoel, Dieter Zapf, and Cary L. Cooper, eds. *Bullying and Harassment in the Workplace: Developments in Theory, Research, and Practice*. 2nd ed. Boca Raton: CRC Press, 2011.

Experiences of Violence and Harassment at Work: A Global First Survey. Geneva: International Labour Organization and Lloyd's Register Foundation, 2022. https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@dgreports/@dcomm/documents/publication/wcms_863095.pdf.

Fitzgerald, Louise F., and Lilia M. Cortina. "Sexual Harassment in Work Organizations: A View from the 21st Century." In *APA Handbook of the Psychology of Women*. Vol. 2, *Perspectives on Women's Private and Public Lives*, edited by Cheryl B. Travis White, Jacquelyn W. Rutherford, Alexandra Williams, Wendi S. Cook, Sarah L. Wyche, and Karen Fraser, 215–34. American Psychological Association, 2018. https://doi.org/10.1037/0000060-012.

Fox, James Alan, and Jack Levin. *Extreme Killing: Understanding Serial and Mass Murder*. 3rd ed. Thousand Oaks: Sage, 2014.

Geck, Carter M., Pamela E. Klassen, Thomas Grimbos, Matthew Siu, and Michael C. Seto. "Violence at Work: An Examination of Aggressive, Violent, and Repeatedly Violent Employees." *Journal of Threat Assessment and Management* 4, no. 4 (2017): 210–29. https://doi.org/10.1037/tam0000091.

Hershcovis, M. Sandy, and Julian Barling. "Towards a Multi-Foci Approach to Workplace Aggression: A Meta-Analytic Review of Outcomes from Different Perpetrators." *Journal of Organizational Behavior* 31, no. 1 (2010): 24–44. https://doi.org/10.1002/job.621.

Hershcovis, M. Sandy, Nick Turner, Julian Barling, Kara A. Arnold, Kathryne E. Dupré, Michelle Inness, Manon Mireille LeBlanc, Niro Sivanathan. "Predicting Workplace Aggression: A Meta-Analysis." *Journal of Applied Psychology* 92, no. 1 (2007): 228–38. https://doi.org/10.1037/0021-9010.92.1.228.

International Labour Organization. *Recommendation Concerning the Elimination of Violence and Harassment in the World of Work (No. 206)*. 2019. Accessed March 10, 2026. https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:R206.

International Labour Organization. *Violence and Harassment Convention, 2019 (No. 190)*. 2019. https://www.ilo.org/dyn/normlex/en/f?p=normlexpub:12100:0::no::p12100_ilo_code:c190.

Jung, Jiwook, Zoltan Lippenyi, and Eunmi Mun. "Workplace Volatility and Gender Inequality: A Comparison of the Netherlands and South Korea." *Socio-Economic Review* 20, no. 4 (2022): 1679–740. https://doi.org/10.1093/ser/mwab026.

Keashly, Loraleigh, and Karen Jagatic. "North American Perspectives on Hostile Behaviors and Bullying at Work." In *Bullying and Harassment in the Workplace*, edited by Ståle Einarsen, Helge Hoel, Dieter Zapf, and Cary L. Cooper, 41–71. Boca Raton: CRC Press, 2011.

Linsley, Paul. *Violence and Aggression in the Workplace*. Boca Raton: CRC Press, 2018.

Neuman, Joel H., and Robert A. Baron. "Aggression in the Workplace: A Social-Psychological Perspective." In *Counterproductive Work Behavior: Investigations of Actors and Targets*, edited by Suzy Fox and Paul E. Spector, 13–40. Washington: American Psychological Association, 2005.

Roscigno, Vincent J. "Social Movement Struggle and Race, Gender, Class Inequality." *Race, Sex & Class* 2, no. 1 (1994): 109–26. https://www.jstor.org/stable/41680099.

Rumler, Fabio, and Johann Scharler. "Labor Market Institutions and Macroeconomic Volatility in a Panel of OECD Countries." European Central Bank Working Paper No. 1005, 2008. https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1005.pdf.

Schat, Aaron C.H., and E. Kevin Kelloway. "Workplace Aggression." In *Handbook of Work Stress*, edited by Julian Barling, E. Kevin Kelloway, and Michael R. Frone, 189–218. Thousand Oaks: Sage, 2005.

Spector, Paul E., and Suzy Fox. "The Stressor–Emotion Model of Counterproductive Work Behavior." In *Counterproductive Work Behavior: Investigations of Actors and Targets*, edited by Suzy Fox and Paul E. Spector, 151–74. Washington: American Psychological Association, 2005.

World Health Organization. *Guidelines on Mental Health at Work*. Geneva: WHO, 2022. https://www.who.int/publications/i/item/9789240053052.

Zapf, Dieter, and Ståle Einarsen. "Bullying in the Workplace: Recent Trends in Research and Practice–An Introduction." *European Journal of Work and Organizational Psychology* 10, no. 4 (2001): 369–73. https://doi.org/10.1080/13594320143000807.

Zapf, Dieter, and Ståle Einarsen. "Mobbing at Work: Escalated Conflicts in Organisations." In *Counterproductive Work Behavior: Investigations of Actors and Targets*, edited by Suzy Fox and Paul E. Spector, 237–70. Washington: American Psychological Association, 2005.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 195–212
https://doi.org/10.31743/recl.19544
Received: 21 January 2026 | Accepted: 9 March 2026 | Published: 31 March 2026

Addressing the Declining Water Level of the Caspian Sea from a Legal Perspective and a Proposal for a New Agreement

Emin Alimusayev
PhD candidate, Baku State University; correspondence address: AZ1148, Academician Zahid Khalilov Street 33, Baku, Azerbaijan; e-mail: eminalimusayev@gmail.com
https://orcid.org/0009-0001-2300-0690

Abstract: The Caspian Sea is currently experiencing a rapid decline in water levels, with a 46% reduction in water-covered area between 2001 and 2024. Considering the environmental and socio-economic impacts of the problem, legal responses remain fragmented. This article examines existing legal frameworks to determine why current instruments fail to mitigate the problem of water-level decline. This study employs a doctrinal and comparative legal analysis of the domestic legislations of the five Caspian littoral states, alongside a review of existing international agreements. The analysis reveals that current instruments are insufficient. Domestic legislation of the Caspian littoral states remains uneven and fragmented. Kazakhstan's Ecological Code serves as a notable model for integrating climate regulation and the response to the decline in water levels in the Caspian Sea into national legislation. While international agreements, such as the Tehran Convention, establish general cooperation principles, they lack binding rules for coordinated river-basin management and climate adaptation. Highlighting a recent surge in regional political will, this paper proposes a new agreement. The proposed agreement introduces binding obligations for reservoir release regimes, minimum environmental flows, and a permanent basin regulatory body. By shifting from ad hoc diplomacy to an integrated legal instrument, the proposal provides a plan for ensuring the socio-economic and environmental security of the Caspian region.

Keywords: Caspian Sea, water level management, water level decline, environmental law, legal response

1. Introduction

The Caspian Sea, being the Earth's largest inland water body, experienced a rapid decline in its water level in the 21st century. This decline poses a significant threat to the ecosystem and surrounding economies. Given the cultural and historical value of the Caspian Sea, its protection requires urgent legal action.

Declining water levels are not new for this region. In recent decades, the Aral Sea and Lake Urmia have experienced severe environmental crises. As one of the largest inland lakes in the 1960s, the Aral Sea underwent a catastrophic transformation by 2006, with its water level dropping by 23 m, surface area shrinking by 74%, and volume decreasing by 90%, mainly due to unsustainable irrigation projects and poor water management policies.[1] Lake Urmia shares a similar fate. Between 1970 and 1997, the decline in Lake Urmia's water level was relatively slow; however, from 1998 to 2018, the lake experienced

[1] Philip Micklin, "The Aral Sea Disaster," *Annual Review of Earth and Planetary Sciences* 35 (2007): 47, https://doi.org/10.1146/annurev.earth.35.031306.140120.

ISSN 2545-384X (Online)

rapid desiccation, resulting in approximately 30% reduction in its total area.[2] The cases of the Aral Sea and Lake Urmia highlight the environmental and socio-economic consequences of large-scale declines in water levels in the region.

Recent studies raised concerns about the drop in the Caspian Sea's water level, as well as its environmental and socio-economic consequences. According to Court *et al.* (2025),[3] between 2001 and 2024, the water-covered area of the Caspian Sea decreased by approximately 46%, with the shoreline retreating over 56 km (especially in the shallow northeastern area), causing severe threats to ecosystems, biodiversity, and coastal infrastructure, necessitating adaptive and transboundary management approaches. Another study[4] finds that between 1993 and 2001, the water level dropped at a rate of about 5.4 cm per year, accelerating to about 8.9 cm per year since 2005. The reasons behind the water level decline are complex, involving both natural and anthropogenic factors. Contrasting with today's downward trend, historical data highlights the Caspian's sensitivity to its drainage system, as the redirection of northern rivers and influx of glacial meltwater previously caused the sea to expand and connect with the Black Sea.[5] It has been demonstrated[6] that climate-driven changes in the Volga River's hydrology are the main cause of the Caspian Sea's water level drop. In addition, a study[7] finds that shifts in the Caspian Sea's wind regime have intensified evaporation and contributed to the decline in water levels. Further research[8] indicates that the Caspian Sea's seasonal circulation and water level changes are mainly caused by changes in winds, river discharge, and air-sea fluxes. In addition to natural causes, human activities such as dam construction, hydrocarbon extraction, and desalination projects have also played a major role in the decline of the Caspian Sea's water level.[9] Since the mid-20th

2 Mehri Shams Ghahfarokhi and Sogol Moradian, "Investigating the Causes of Lake Urmia Shrinkage: Climate Change or Anthropogenic Factors?," *Journal of Arid Land* 15, no. 4 (2023): 424, https://doi.org/10.1007/s40333-023-0054-z.

3 Rebecca Court et al., "Rapid Decline of Caspian Sea Level Threatens Ecosystem Integrity, Biodiversity Protection, and Human Infrastructure," *Communications Earth & Environment* 6 (2025): 261, https://doi.org/10.1038/s43247-025-02212-5.

4 Jianli Chen et al., "Caspian Sea Level Change Observed by Satellite Altimetry," *Remote Sensing* 15, no. 3 (2023): 703, https://doi.org/10.3390/rs15030703.

5 Sifan A. Koriche et al., "What Are the Drivers of Caspian Sea Level Variation during the Late Quaternary?," *Quaternary Science Reviews* 283 (2022): 107457, https://doi.org/10.1016/j.quascirev.2022.107457.

6 Elnur Safarov, Said Safarov, and Emil Bayramov, "Changes in the Hydrological Regime of the Volga River and Their Influence on Caspian Sea Level Fluctuations," *Water* 16, no. 12 (2024): 1744, https://doi.org/10.3390/w16121744.

7 Elnur Safarov et al., "Impact of Changes in the Wind Regime on the Caspian Sea Level Fluctuation and Its Relationship with SOI and NAO," *Scientific Reports* 15 (2025): 36380, https://doi.org/10.1038/s41598-025-20346-6.

8 Rashit A. Ibrayev et al., "Seasonal Variability of the Caspian Sea Three-Dimensional Circulation, Sea Level and Air-Sea Interaction," *Ocean Science* 6, no. 1 (2010): 311–29, https://doi.org/10.5194/os-6-311-2010.

9 Aida Amangeldina, "The Caspian Sea is Under Threat of Desertification: What Are the Causes and Consequences?," Central Asia Climate Information Portal, November 12, 2024, accessed March 19, 2026, https://centralasiaclimateportal.org/publications/the-caspian-sea-is-under-threat-of-desertification-what-are-the-causes-and-consequences.

century, the Caspian Sea's long-term water decline has been partly driven by human activities that reduce the freshwater entering the basin, in addition to climate-related changes in evaporation and precipitation.[10] Furthermore, shipping operations and weak enforcement of environmental regulations have intensified emissions, pollution, and evaporation, contributing to the drop in water levels.[11] These factors led to a decline in the Caspian Sea level, raising serious concerns about its future. Further research[12] predicts that, due to climate change and increasing evaporation, the water level will drop by up to about 14 m by 2100, causing major ecological and economic impacts even under low-carbon emission scenarios.

Despite growing concern, a limited number of papers have explored clear policy and legal solutions to the Caspian Sea's environmental challenges. UNEP working paper[13] warns of the rapid decline of the Caspian Sea and urges coordinated scientific research, transboundary adaptation planning, and institutional cooperation among all Caspian littoral states to protect coastal ecosystems and infrastructure from the impacts of water-level decline. According to another policy brief,[14] addressing the Caspian Sea's declining water level requires coordinated regional water-conservation efforts, scientific cooperation, and active engagement of the international community. Further study[15] recommended regional cooperation on scientific monitoring, water management, and legal adaptation to mitigate the decline in water levels.

Addressing the crisis of declining Caspian Sea water levels requires more than just scientific monitoring and research; it requires a unified legal response. This study fills this gap by analyzing the domestic legislative frames of Caspian littoral states and international legal instruments to identify systemic gaps. Ultimately, it proposes a new international agreement designed to harmonize regional efforts and mitigate both anthropogenic and natural factors.

---

10 Hamid Lahijani et al., "Caspian Sea Level Changes during Instrumental Period, Its Impact and Forecast: A Review," *Earth-Science Reviews* 241 (2023): 104428, https://doi.org/10.1016/j.earscirev.2023.104428.

11 Black Sea Institute, "Aral Sea Syndrome: Why Is the Caspian Sea Shrinking?," August 21, 2024, accessed March 19, 2026, https://blacksealaw.org/aral-sea-syndrome-why-is-the-caspian-sea-shrinking/.

12 Rohit Samant and Matthias Prange, "Climate-Driven 21st Century Caspian Sea Level Decline Estimated from CMIP6 Projections," *Communications Earth & Environment* 4, no. 1 (2023): 297, https://doi.org/10.1038/s43247-023-01017-8.

13 United Nations Environment Programme, "Caspian Sea Fluctuations and Climate Change" (Working Paper, UNEP DHI Partnership – Centre on Water and Environment, Nairobi, 2024), https://unepdhi.org/wp-content/uploads/sites/2/2024/11/Caspian_Sea_working_paper.pdf.

14 Allan Mustard, Aizhan Abilgazina, and Akbota Karibayeva, *The Silent Threat of Falling Caspian Sea Levels: A Caspian Policy Center Policy Brief* (Washington: Caspian Policy Center, 2021), https://api.caspianpolicy.org/media/ckeditor_media/2021/11/04/the-silent-threat-of-falling-caspian-sea-levels.pdf.

15 Rodrigo Labardini and Nazrin Baghirova, *Desiccation in the Caspian Sea: On the Need to Implement Domestic and Regional Countermeasures, Analytical Policy Brief* (Baku: Institute for Development and Diplomacy, 2023), https://idd.az/media/2024/01/12/idd_policy_brief_-_labardini-baghirova_22_december.pdf?v=1.1.

2. Materials and Methods

The main thesis of this article is that the existing national and international legal frameworks are insufficient to address the crisis of the Caspian Sea's water level decline. Therefore, a unified and legally binding international agreement is necessary. To test this thesis, this study employs a combination of doctrinal and comparative legal analyses. The research is structured into three phases: an evaluation of domestic legislation across littoral states, an assessment of existing international legal instruments and the formulation of a *de lege ferenda* proposal for a new regional agreement.

The comparative legal analysis focuses exclusively on the five littoral states of the Caspian Sea: Azerbaijan, Russia, Kazakhstan, Turkmenistan, and Iran. This scope is deliberately restricted to these nations because they hold exclusive sovereign rights, jurisdiction and the primary legal burden for environmental protection within their respective sectors under the international agreements. While international rivers significantly impact the sea's volume, the legal mandate to establish a unified policy rests strictly with the littoral states.

To move beyond a general description of foreign legal acts, this study evaluates the domestic legal frameworks of the littoral states against a specific catalog of regulatory factors. The analysis investigates how each national system addresses the following legal factors: constitutional and general environmental frameworks, water management, climate regulation, and implementation challenges. This factor-based approach allows the comparative analysis to function not only as a descriptive survey of foreign legal orders, but as a diagnostic tool identifying which regulatory elements are present, absent, or underdeveloped across the littoral states and which national models are most suitable as patterns for the proposed agreement.

The primary sources of this research include: national legislation (official legal acts taken from platforms such as "e-qanun.az," "adilet.kz," "consultant.ru," "minjust.gov.tm"), international legal instruments (such as agreements, conventions, memoranda), and decisions of international courts (such as Pulp Mills on the River Uruguay [Argentina v. Uruguay; 2010] and Gabčíkovo-Nagymaros Project [Hungary v. Slovakia; 1997]). Secondary sources include scientific research papers, policy documents and earth science literature on Caspian hydrological dynamics.

The study acknowledges limitations in the accessibility of updated legal regulations in certain jurisdictions (especially Iran) and in relying on translations of national legal acts.

3. Results and Discussion

3.1. Analysis of National Legal Frameworks

This section analyzes the legal dimensions of the Caspian Sea's water level decline by examining how existing national legislative frameworks regulate the natural and anthropogenic drivers of the crisis. While all littoral states possess foundational environmental laws, their approaches to climate regulation and water management vary in scope and enforceability.

3.1.1. The Republic of Azerbaijan

The Constitution[16] plays a role in Azerbaijan's legislative framework primarily by setting the general principles and key objectives for environmental regulation. Article 39 establishes the right to a healthy environment and mandates the state to maintain ecological balance, while Article 78 enshrines the duty to protect the environment.

The central legislative act is the Law "On Environmental Protection."[17] While it addresses broad concepts, such as ecological balance and economic protection tools, it lacks specific enforcement mechanisms for climate regulation. Notably, Article 49 ("Protection of the Climate and Ozone Layer") functions as a declarative provision, deferring to international agreements rather than establishing domestic obligations. Similarly, while the Law "On the Protection of Atmospheric Air" prohibits projects damaging to the climate, it fails to define specific criteria for what constitutes "damage." Further laws on "On the Use of Renewable Energy Sources in the Production of Electric Energy," "On Energy," and "On Electro-energy" include provisions to promote renewable energy sources and reduce greenhouse gas emissions, without setting clear obligations.

The Water Code[18] designates the Azerbaijani sector of the Caspian Sea as part of the State Water Fund (Article 5). However, it does not establish a dedicated regulatory regime for the Caspian Sea; instead, it relies on general national acts. Although the "National Strategy on the Efficient Use of Water Resources"[19] obligates authorities to evaluate climate impacts on the Caspian, Azerbaijan currently lacks a dedicated climate law,[20] addressing the issue primarily through non-binding policy strategies.

3.1.2. The Russian Federation

Russia is a Caspian littoral state that controls the Volga River, the primary water source of the Caspian Sea. Therefore, the analysis of its legislation is crucial. The Constitution (1993) establishes the right to a favorable environment (Article 42) and the obligation to preserve natural wealth (Article 58)[21] of the Russian Federation, and determines the right to a favorable environment as a human right. Furthermore, Article 58 obligates people to preserve nature and the environment, and to carefully manage natural resources.

The Federal Law "On Environmental Protection"[22] (2002) serves as the core framework. While it sets standards for monitoring and liability, it does not specifically include

16 Constitution of the Republic of Azerbaijan (1995), https://e-qanun.az/framework/897.

17 Law of the Republic of Azerbaijan No. 678-IQ "On Environmental Protection" (1999), https://e-qanun.az/framework/3852.

18 Water Code of the Republic of Azerbaijan (1997), https://e-qanun.az/framework/46940.

19 National Strategy on the Efficient Use of Water Resources (2024), https://e-qanun.az/framework/58119.

20 Emin Alimusayev, "Analysis of Legal Challenges in Climate Regulation of Azerbaijan and Proposal for Climate Law," *Law. Human. Environment* 16, no. 4 (2025): 42–58, https://doi.org/10.31548/law/4.2025.42.

21 Constitution of the Russian Federation (1993), https://www.constitution.ru/en/10003000-01.htm.

22 Federal Law of the Russian Federation No. 7-FZ "On Environmental Protection" (2002), https://www.consultant.ru/document/cons_doc_LAW_34823/.

climate regulation. Water management is governed by the Water Code,[23] which establishes "basin districts" (Article 28) and mandates "schemes of complex use" (Article 33). Crucially, Article 45 regulates reservoir operations. While the legal basis for monitoring exists, the framework is often criticized for ineffectiveness. According to Sivakov[24] (2020), gaps in the legal framework enable corrupt practices that hinder the preservation of water bodies. Another research analyzed how ecosystem services are currently neglected in Russia's water policy and argues for their institutionalization to address environmental problems.[25] Furthermore, Venitsianov (2019) noted that key challenges in Russian water protection include ineffective wastewater treatment, deteriorated monitoring systems, outdated legislation, and a failure to transition to the best available technologies.[26]

Regarding climate, Russia adopted the Federal Law "On Limiting Greenhouse Gas Emissions"[27] in 2021. However, it is often criticized for lacking clarity, being vague, and framework-based.[28] Further research refers to Russia's climate legislation as "climate obstructionism."[29] According to another article, the absence of a comprehensive climate law in Russia undermines effective climate governance, necessitating the adoption of a strong climate law.[30]

3.1.3. The Republic of Kazakhstan

Kazakhstan represents the most advanced legislative model among the littoral states. The Constitution (Articles 31 and 38)[31] establishes the foundation, which the 2021 Ecological Code operationalize.[32]

---

23 Water Code of the Russian Federation No. 74-FZ (2006), https://www.consultant.ru/document/cons_doc_LAW_60683/.

24 Dmitry O. Sivakov, Viacheslav V. Sevalnev, and Yuri V. Truntsevsky, "Use and Protection of Water Bodies: Corruption Cases," *E3S Web of Conferences* 203 (2020): 02016, https://doi.org/10.1051/e3sconf/202020302016.

25 Timofey D. Moiseev and Sofia T. Garipova, "Water Use and Ecosystem Services: A Case of Russia," *Environmental Dynamics and Global Climate Change* 13, no. 2 (2022): 60–69, https://doi.org/10.18822/edgcc105930.

26 Yevgeniy V. Venitsianov, "Modern Problems of Water Protection in Russia," *IOP Conference Series: Earth and Environmental Science* 321 (2019): 012033, https://doi.org/10.1088/1755-1315/321/1/012033.

27 Federal Law of the Russian Federation No. 296-FZ "On Limiting Greenhouse Gas Emissions" (2021), https://www.consultant.ru/document/cons_doc_LAW_388992/.

28 Natalia G. Zhavoronkova and Vyacheslav B. Agafonov, "The Role of National Climate Law in Ensuring the 'Energy Transition,'" *Lex Russica* 17, no. 2 (2022): 151–62, https://doi.org/10.17803/1994-1471.2022.135.2.151-162.

29 Marianna Poberezhskaya and Ellie Martus, "Climate Obstruction in Russia: Surviving a Resource-Dependent Economy, an Authoritarian Regime, and a Disappearing Civil Society," in *Climate Obstruction across Europe*, eds. Robert J. Brulle, J. Timmons Roberts, and Miranda C. Spencer (New York: Oxford University Press, 2024), 214–42, https://doi.org/10.1093/oso/9780197762042.003.0009.

30 Aleksey Anisimova, Yulia Isakova, and Olga Volkonskaya, "Trends and Prospects for the Formation of a National Model of Climate Legislation (Using the Russian Federation as an Example)," *Vniversitas Jurídica* 74 (2025), https://doi.org/10.11144/Javeriana.vj74.tpfn.

31 Constitution of the Republic of Kazakhstan (1995), https://adilet.zan.kz/eng/docs/K950001000_.

32 Environmental Code of the Republic of Kazakhstan No. 400-VI (2021), https://adilet.zan.kz/eng/docs/K2100000400.

Unlike its neighbors, Kazakhstan's Ecological Code includes a dedicated Chapter 19 regarding the Northern Caspian Sea. Recognizing that this shallow zone is most vulnerable to water-level decline, the Code establishes a "State Conservation Area" with strict prohibitions on destructive activities such as water discharge and polluting construction. Furthermore, Chapter 20 integrates climate change directly into national law, establishing carbon budgeting, quota-trading systems, and a target to reduce emissions by 15% by 2030.

In 2025, Kazakhstan further strengthened its regime with the adoption of a new Water Code,[33] which introduces the concept of "water security" into national legislation.[34] A key innovation is Article 39, which defines "ecological runoff" as a mandatory proportion of river runoff intended to preserve river, lake, and marine ecosystems, and to be left in nature. It emphasizes ecological runoff as a priority that must be respected. The Code mandates comprehensive water planning, requiring both national and river-basin management plans. Chapter 2 is dedicated to the water sector's adaptation to climate change. This chapter establishes a system for preventing and managing floods and other harmful water-related effects, and defines drought adaptation measures, including monitoring, alternative water sources, and water conservation and storage. Despite these robust laws, challenges remain. According to the UNDP article[35] (2025), fragmented governance remains the biggest obstacle in Kazakhstan's water management. Furthermore, Sopykhanova *et al.* (2023) examine how legal regulation and state policy in Russia and Kazakhstan remain fragmented and insufficiently aligned with the United Nations 2030 Agenda for Sustainable Development, particularly in environmental protection and natural-resource management.[36]

3.1.4. Turkmenistan

The Constitution of Turkmenistan guarantees the right to a healthy environment and obliges the state to ensure the sustainable use of resources.[37] The Law "On Nature Preservation"[38] addresses climate protection in Article 47, setting objectives to stabilize greenhouse gas concentrations. While there is currently no dedicated climate law, a draft "Law on Climate Change" was presented in 2025.[39]

---

33 Water Code of the Republic of Kazakhstan No. 178-VIII (2025), https://adilet.zan.kz/eng/docs/K2500000178.

34 Uchet.kz, "New Water Code Entered into Force," June 10, 2025, accessed March 19, 2026, https://uchet.kz/news/novyy-vodnyy-kodeks-vstupil-v-silu/.

35 Yerassyl Kalikhan, "Water Management in Kazakhstan: A Systems Approach for a Secure Future," United Nations Development Programme, March 18, 2025, accessed March 19, 2026, https://www.undp.org/kazakhstan/blog/water-management-kazakhstan-systems-approach-secure-future.

36 Assel Sopykhanova et al., "Problems of Legal Regulation and State Policy Measures Related to Nature Management in the Framework of Achieving the SDGs: Examples from Russia and Kazakhstan," *Sustainability* 15, no. 2 (2023): 1042, https://doi.org/10.3390/su15021042.

37 Constitution of Turkmenistan (2016), https://minjust.gov.tm/ru/hukuk/merkezi/hukuk/1.

38 Law of Turkmenistan "On Nature Protection" (2014), https://minjust.gov.tm/ru/hukuk/merkezi/hukuk/154.

39 State News Agency of Turkmenistan, "Presentation of the Draft Law 'On Climate Change' Was Held in Ashgabat," Turkmenistan: Golden Age, June 6, 2024, accessed March 19, 2026, https://aarhusashgabat.org/blog/v-ashhabade-sostoyalas-prezentacziya-zakonoproekta-ob-izmenenii-klimata/.

The Water Code[40] includes the Turkmen sector of the Caspian Sea in the State Water Fund, but lacks specific provisions for managing water-level fluctuations. International observers note a significant gap between policy and practice. According to the UN Economic Commission, weak enforcement of existing laws remains one of the biggest challenges in Turkmenistan's environmental legislation. In addition, the NAP Global Network[41] highlights the absence of a permanent technical secretariat and a formal legal framework to systematically mainstream adaptation priorities into sectoral planning, particularly within the water and agriculture industries, which remain the biggest obstacles to Turkmenistan's climate regulation. Further research[42] identifies significant gaps between Turkmenistan's high-level climate strategies and the specific regulatory mechanisms needed for effective enforcement on the ground.

3.1.5. The Islamic Republic of Iran

Iran's Constitution (Article 50)[43] declares environmental protection a public duty and strictly prohibits activities that cause irreparable damage. While Iran lacks a dedicated climate law, it adopted a "National Climate Change Management Plan" in 2025 to bridge this gap, though scholars continue to call for binding legislation.[44]

Water regulation is regulated by the Water Law[45] and the Law on Equal Distribution of Water.[46] While these laws do not include specific provisions on the Caspian Sea's water level, Voynova (2023) notes that Iran's environmental legislation has gradually evolved into a comprehensive framework aimed at protecting the Caspian Sea's water resources, biodiversity, and marine environment across six historical stages.[47] Furthermore, corruption and weak enforcement of laws hinder the effectiveness of water regulation in Iran.[48]

---

40 Water Code of Turkmenistan (2016), https://minjust.gov.tm/ru/hukuk/merkezi/hukuk/527.

41 Bunafsha Mislimshoeva et al., *Institutional Analysis of the Current National System and Processes Related to Climate Change in Turkmenistan* (International Institute for Sustainable Development, 2021), https://napglobalnetwork.org/wp-content/uploads/2021/06/napgn_en_2021_institutional-analysis-of-the-current-national-system-and-processes-related-to-climate-change-in-turkmenistan.pdf.

42 Yolbars Kepbanov, *Legal Protection of Climate in Turkmenistan: Assessment of the Current Situation and Development Prospects: Research Report in Sociology of Law*, 2023:4 (Lund: Lund University, 2023), https://www.researchgate.net/publication/375923460.

43 Constitution of the Islamic Republic of Iran (1979), https://www.shora-gc.ir/en/news/87/constitution-of-the-islamic-republic-of-iran-full-text.

44 Ali Khalili, "Climate Changes and Iran's 7th Development Plan at a Glance," *Journal of Agricultural Meteorology* 11, no. 2 (2023): 1–3, https://doi.org/10.22125/agmj.2023.186488.

45 Iran Water Law and the Manner of Water Nationalization (1968), https://www.cawater-info.net/bk/water_law/pdf/iran1968.pdf.

46 Law of Fair Water Distribution (1982), https://fa.wikisource.org/wiki/Law_of_Fair_Water_Distribution.

47 Maria V. Voynova, "Main Stages of Developing Environmental Legislation of Islamic Republic of Iran on Environmental Protection of Caspian Sea," *Oil and Gas Technologies and Environmental Safety* 2 (2023): 69–82, https://doi.org/10.24143/1812-9498-2023-2-69-82.

48 Kamyar Kayvanfar, "Iran's Water Crisis: Historical Roots, Ideological Dimensions and Policy Challenges," ORF Middle East, November 12, 2025, accessed March 19, 2026, https://orfme.org/expert-speak/irans-water-crisis-historical-roots-ideological-dimensions-and-policy-challenges/.

Table. Comparative analysis of national legislations of Caspian littoral states

State	Key legislative acts	Primary legal challenges
Azerbaijan	The Constitution (Articles 39, 78); The Water Code; Law "On Environmental Protection."	No dedicated laws on climate or the Caspian Sea water level decline; vague provisions.
Russia	Constitution (Articles 42, 58); Federal Law "On Environmental Protection"; The Water Code Federal Law N296-FZ "On Limiting GHG Emissions."	Legislation is framework-based and lacks clarity on enforcement; deteriorated monitoring systems; gaps enable corrupt practices.
Kazakhstan	Constitution (Articles 31, 38); The Ecological Code; The Water Code.	Fragmented regulation.
Turkmenistan	Constitution (Articles 15, 53); Law on Nature Preservation; The Water Code; Draft Law "On Climate Change."	Institutional void; enforcement gap.
Iran	Constitution (Article 50); National Climate Change Management Plan; Water Law; Law on Equal Distribution of Water.	No dedicated climate law exists; general water laws do not include specific provisions addressing fluctuations in the Caspian water level; corruption and weak enforcement hinder the effectiveness of existing environmental frameworks.

Source: systematized by the author.

3.2. Legal Status of the Caspian Sea and Environmental Regulation Agreements

Historically, the Caspian Sea was regulated by bilateral agreements between Persia and the Russian Empire. With the collapse of the Soviet Union in 1991, three new littoral states emerged. As Azerbaijan, Kazakhstan, and Turkmenistan regained their independence, debates on the legal nature of the Caspian Sea were sparked. Due to the different interests of the littoral states, total consensus was not easily reached. In the early stages of discussions, northern states signed a series of bilateral agreements.

The existing legal framework of the Caspian Sea rests on two distinct pillars: the 2018 Convention,[49] which serves as a political constitution for legal status, and the 2003 Tehran Convention,[50] which serves as the primary environmental framework for ecological cooperation. In 2018, the Convention on the Legal Status of the Caspian Sea was signed by all littoral states. This Agreement created a *sui generis* legal status. The Convention divides the Caspian Sea into 15-mile sovereign territorial waters and 10-mile exclusive

[49] Convention on the Legal Status of the Caspian Sea, signed August 12, 2018, https://tehranconvention.org/system/files/web/convention_on_the_legal_status_of_the_caspian_sea_en.pdf.

[50] Framework Convention for the Protection of the Marine Environment of the Caspian Sea, signed November 4, 2003, https://tehranconvention.org/system/files/tc-interim-secretariat/tehran_convention_text_final_pdf.pdf.

fishing zones for each state, while treating the central water surface as a common area for navigation. For seabed and subsoil, delimitation into national sectors must be agreed upon by the states. Despite the Convention's provisions for the general protection of the environment, it does not specifically address the decline in water levels in the Caspian Sea. Furthermore, in scientific literature, this Agreement is often criticized for unresolved legal and practical questions that require further clarification and could lead to interstate tensions.[51]

The Tehran Convention, formally known as the Framework Convention for the Protection of the Marine Environment of the Caspian Sea, was adopted in 2003 and became enforceable in 2006. It is the first legally binding, multilateral environmental agreement among the five Caspian littoral states. It establishes a framework for preventing pollution, protecting biodiversity, and promoting regional cooperation. The Preamble of the Convention notes that the contracting parties are mindful of the dangers to the marine environment of the Caspian Sea and of its unique hydrographic and ecological characteristics, particularly in relation to sea level fluctuations. Article 3 defines the scope of the Convention, stipulating that it shall apply to the marine environment of the Caspian Sea, taking into account fluctuations in water levels and pollution from land-based sources. Article 11 states that the contracting parties shall take all appropriate measures to reduce the possible negative impact of anthropogenic activities aimed at mitigating the consequences of the sea level fluctuations on the Caspian Sea ecosystem. Furthermore, Article 16 of the Convention obligates the parties to collaborate on scientific research and practical measures to mitigate the environmental and socio-economic impacts of Caspian Sea level changes. However, despite the acknowledgment of the risk of water level fluctuations in the Convention, many of its obligations remain ambiguous, lacking concrete enforcement mechanisms, binding targets, and detailed implementation procedures. As a result, state compliance largely depends on political will, which has limited the Convention's effectiveness in addressing the accelerating environmental challenges facing the Caspian Sea. Moreover, given that climate-related factors largely drive contemporary Caspian Sea-level decline, the Convention lacks specific provisions addressing climate change impacts or adaptation measures, further limiting its practical effectiveness.

In 1994, the Coordinating Committee on Hydrometeorology and Pollution Monitoring of the Caspian Sea[52] (CASPCOM) was established by the littoral states. Its main purpose is to coordinate, standardize, and improve regional hydrometeorological research and pollution monitoring in the Caspian Sea. Furthermore, CASPCOM regularly issues bulletins[53] on the Caspian Sea water level. In 2013, the Memorandum of Understanding between CASPCOM and the interim Secretariat of the Tehran Convention was signed.

---

51 Michał Pietkiewicz, "Legal Status of Caspian Sea – Problem Solved?," *Marine Policy* 123 (2020): 104321, https://doi.org/10.1016/j.marpol.2020.104321.

52 Coordinating Committee on Hydrometeorology and Pollution Monitoring of the Caspian Sea (CASPCOM), *Statute of the Coordinating Committee on Hydrometeorology and Pollution Monitoring of the Caspian Sea* (2025), http://www.caspcom.com/wp-content/uploads/2025/05/Statute_CASPCOM_eng.pdf.

53 Co-Ordination Committee for Hydrometeorology and Pollution Monitoring of the Caspian Sea (CASPCOM), *Information Bulletin on the State of the Caspian Sea Level No. 30* (2025), http://www.caspcom.com/wp-content/uploads/2025/12/CASPCOM-Bulletin-No.30.pdf.

The Memorandum is intended to facilitate cooperation in addressing the environmental challenges of the Caspian Sea, such as pollution, habitat loss, and the effects of climate change. In 2016, the Agreement on Cooperation in the Field of Hydrometeorology of the Caspian Sea was signed. It established a binding framework for cooperation among the five Caspian littoral states in the observation, monitoring, forecasting and exchange of hydrometeorological and environmental data related to the Caspian Sea.

In 2014, littoral states signed an agreement[54] on cooperation in cases of emergency. It aims to establish a cooperative framework for preventing and responding to natural and anthropogenic disasters in the Caspian Sea region. It establishes procedures for requests, transit, costs, liability, and operational cooperation, while respecting national laws and international obligations. Furthermore, in 2014, another Agreement[55] on the conservation and sustainable use of the Caspian Sea's aquatic biological resources was signed. This Agreement commits the five Caspian states to cooperate to conserve and sustainably use aquatic biological resources through ecosystem-based management, scientific research, data sharing, and combating illegal fishing, while enabling economic activities.

Beyond regional accords, the 1997 UN Convention on the Law of the Non-Navigational Uses of International Watercourses[56] provides a critical normative benchmark for the proposed agreement. Although the Caspian littoral states are not parties to this instrument, its core principles of "equitable and reasonable utilization" (Article 5) and the "obligation not to cause significant harm" (Article 7) represent customary international law.

Furthermore, international jurisprudence and general principles of international law offer essential precedents for managing shared water crises. The principle of good neighborliness obliges states to exercise their sovereign rights over shared natural resources in a manner that does not cause significant harm to neighboring states. For example, in the Pulp Mills on the River Uruguay (2010) case,[57] the International Court of Justice established that states sharing international waterways bear binding procedural obligations before authorizing activities capable of causing transboundary environmental harm. Similarly, the Gabčíkovo-Nagymaros Project (1997) ruling[58] emphasizes the need for sustainable development and ecological necessity when managing shared river systems. Integrating these judicial standards into the Caspian legal framework would provide the mechanisms currently missing from the Tehran Convention, ensuring that any anthropogenic activities affecting water levels are subject to rigorous, multi-state legal scrutiny.

54 Agreement on Cooperation in the Field of Prevention and Elimination of Emergency Situations in the Caspian Sea, signed September 29, 2014, https://e-qanun.az/framework/28996.

55 Agreement on the Conservation and Sustainable Use of Aquatic Biological Resources of the Caspian Sea, signed September 29, 2014, https://tehranconvention.org/system/files/web/bioresources_2014.pdf.

56 Convention on the Law of the Non-navigational Uses of International Watercourses, signed May 21, 1997, https://legal.un.org/ilc/texts/instruments/english/conventions/8_3_1997.pdf

57 ICJ Judgment of 20 April 2010, Pulp Mills on the River Uruguay (Argentina v. Uruguay), 135–20100420-JUD-01–00-EN, p. 14, https://www.icj-cij.org/case/135.

58 ICJ Judgment of 25 September 1997, Gabčíkovo-Nagymaros Project (Hungary/Slovakia), 092–19970925-PRE-01–00-EN, p. 7, https://www.icj-cij.org/case/92.

3.3. Necessity of a New International Agreement

As mentioned above, the decline of the Caspian Sea's water level is scientifically proven and an intensifying crisis for the region. Despite the Caspian historically experiencing natural fluctuations, recent scientific evidence indicates that the current trend represents an accelerating decline rather than a cyclical pattern. Natural (climate change altering the balance between evaporation and precipitation) and anthropogenic (dam construction, hydrocarbon extraction, desalination, shipping operations, and weak environmental regulations) factors are jointly reshaping the hydrological balance of the Caspian Sea. In this context, reliance on the existing legal instruments is no longer sufficient.

Existing international legal instruments regulating the Caspian Sea establish important principles of sovereignty, delimitation, and cooperation. However, they do not contain binding and efficient rules specifically designed to address water-level decline, coordinated river-basin management, or climate regulation. At the national level, the littoral states have adopted environmental and water legislation to address various aspects of environmental regulation. However, these national legislations face significant challenges of implementation, enforcement, and institutional capacity. In most Caspian states, climate change is addressed primarily through policy rather than through comprehensive, binding climate legislation. Kazakhstan's Ecological Code constitutes a notable exception, as it integrates environmental protection with climate regulation and provides a more advanced normative basis for addressing the impacts of the Caspian Sea's decline. Overall, domestic legal regimes remain territorially limited and uneven, whereas the causes and consequences of the Caspian Sea's water level decline are regional and transnational in nature. The absence of specialized provisions reveals a clear normative and institutional gap between the scale of the environmental risk and the current legal response.

The problem's transnational character further underscores the need for a new agreement. As the Caspian Sea is a closed basin, any alteration in inflows or coastal development within one littoral state inevitably affects the ecological balance of the other littoral states. As discussed above, water level decline causes significant environmental, economic, and political impacts to the region, including biodiversity loss, salt storms,[59] reduced shipping and infrastructure capacity, fisheries collapse, and border disputes.[60] These impacts cannot be prevented or mitigated through unilateral action, but require coordinated collective action. As a result, the decline in the Caspian water level constitutes not only an environmental problem, but also a matter of regional development, economic security, and social stability.

Recognizing the environmental and geopolitical risks posed by the declining water level, the leaders of the littoral states have addressed the issue on various occasions.

[59] Aigerim Duisembay, "How the Shallowing of the Caspian Sea Affects the Economy of Coastal Regions and Logistics," Kazinform, January 7, 2026, accessed March 19, 2026, https://www.inform.kz/ru/kak-obmelenie-kaspiya-vliyaet-na-ekonomiku-pribrezhnih-regionov-i-logistiku.

[60] Umud Shokri, "Caspian Sea Decline Harms Iran and Raises Regional Tensions," Stimson Center, November 7, 2025, accessed March 19, 2026, https://www.stimson.org/2025/caspian-sea-decline-harms-iran-and-raises-regional-tensions/.

For example, on October 18, 2025, the President of Azerbaijan, Ilham Aliyev, called on the Caspian littoral states to strengthen cooperation, exchange scientific data and develop coordinated measures in response to the rapidly declining level of the Caspian Sea. On September 8, 2025, the President of Kazakhstan, Kassym-Jomart Tokayev, announced the launch of an international program calling on Caspian littoral states to unite scientific efforts and policy measures to save the Caspian Sea from its rapidly declining water levels. Similarly, the President of Turkmenistan, Serdar Berdimuhamedov, highlighted the crisis of declining water levels and initiated the Caspian Environmental Initiative, a platform for dialogue on protecting the Caspian ecosystem. Moreover, Russia's Prime Minister, Mikhail Mishustin, stressed that Russia is taking active measures in response to the lowering water levels and that a joint working group with Azerbaijan has been established to address the problem. In addition, Iran's Foreign Minister urged the five Caspian Sea littoral states to adopt a unified, scientific approach to address the lake's receding water levels caused by climate change, dam construction, and reduced river inflows.

A number of studies addressed the regulation of shared water bodies. Mitchell and Zawahri[61] showed that treaty features such as monitoring, information exchange, and enforcement provisions are statistically associated with better cooperation and reduced conflict over shared rivers. In addition, the UN Economic Commission for Europe identifies the existence of joint bodies, mechanisms, or commissions as a core indicator of whether transboundary water cooperation is operationally effective.[62] These establishments foster communication, data exchange, joint planning, and dispute resolution. Further study finds that river commissions and similar institutional mechanisms facilitate long-term cooperation, build technical knowledge and routinize structured interaction among riparian states.[63] Regimes that rely only on political declarations or *ad hoc* cooperation have proven insufficient to address complex, long-term, and climate-driven challenges. Moreover, principles of international environmental law, including the duty to cooperate, the obligation to prevent harm, the precautionary principle and intergenerational equity, support the adoption of proactive and coordinated measures in situations of serious and uncertain risk.

Considering all the above, a specialized international agreement on Caspian Sea water level management and climate adaptation is legally and scientifically justified. Such an instrument would complement existing frameworks by providing binding, operational rules, institutional capacity, and adaptive regulation tools necessary to respond effectively to the decline of the Caspian Sea.

---

61 Sara M. Mitchell and Neda A. Zawahri, "The Effectiveness of Treaty Design in Addressing Water Disputes," *Journal of Peace Research* 52, no. 2 (2015): 187–200, https://doi.org/10.1177/0022343314559623.

62 United Nations Economic Commission for Europe, *Progress on Transboundary Water Cooperation under the Water Convention: Third Report on Implementation* (2024), https://unece.org/sites/default/files/2024-12/-2417627_E_PDF_WEB.pdf.

63 Dinara R. Ziganshina, "Institutional Mechanisms for Preventing and Resolving Cross-Border Water Disputes," *AJIL Unbound* 115 (2021): 195–200, https://doi.org/10.1017/aju.2021.20.

3.4. Proposal for a New Agreement

Previous sections analyzed the national legislations of the Caspian littoral states and international agreements regulating various aspects of the Caspian Sea, as well as the necessity of a new agreement. In light of the legal challenges identified above, this article proposes drafting a dedicated agreement on Caspian Sea water-level management. Such an agreement should be considered not as a replacement of the above-mentioned conventions, but as a complementary and operational framework that transforms general provisions regarding the water level of the Caspian Sea into concrete and enforceable international obligations. Drawing upon the functional comparative analysis conducted in the previous sections, this new agreement should utilize the most advanced regulatory elements found in the domestic legal frameworks of the littoral states (such as Chapter 19 of Kazakhstan's Ecological Code) as baseline patterns for regional standards.

The proposed agreement should define a clear scope that encompasses the Caspian Sea and all transboundary activities that significantly affect its hydrological regime, including river inflows, reservoir operations, and coastal development. Guided by the customary international law principles of equitable and reasonable utilization and the obligation not to cause significant harm, key obligations should include consultation and consent for new infrastructure, minimum environmental flows and reservoir release regimes, coordinated reservoir operations, adaptive planning (including climate dimension), and climate mitigation measures, as well as financing mechanisms. These obligations would ensure that new projects do not undermine basin stability, that reservoirs are operated collectively to protect water levels and ecosystems, that climate risks are addressed through both mitigation and adaptation, and that sufficient financial resources are available to support implementation. In addition, given the primary role of the Paris Agreement (2015) in global climate response, the proposed agreement focuses more on the anthropogenic drivers of the water-level decline problem. Nevertheless, considering the legal challenges in the climate legislations of the littoral states, it should include climate mitigation measures.

Joint monitoring (similar to the CASPCOM model) is crucial to ensure the continuous collection, verification, and transparent exchange of hydrological, climatic, and reservoir data, providing a common, scientific basis for decision-making and early warning of critical water-level declines. Such a system would enhance trust among the parties and enable coordinated, evidence-based responses to potential risks. The proposed agreement should also establish a permanent basin regulatory body to supervise implementation, coordinate policies, and manage technical cooperation. In addition, it must include robust compliance and verification mechanisms to ensure compliance with agreed-upon obligations, as well as clear and effective dispute-resolution procedures to manage disagreements.

The proposed agreement would address the decline in water levels by defining obligations for the Caspian littoral states to protect the basin's ecosystem. Through these obligations and institutional mechanisms, it would enable early detection of risks, ensure accountability, and promote long-term, cooperative responses to the water-level decline problem. In this way, the proposed agreement would provide the legal and institutional

mechanisms required to move from fragmented national responses to an integrated and adaptive regional regulation framework for the Caspian Sea.

4. Conclusion

The declining water levels of the Caspian Sea are no longer a scientific forecast; it is today's regional crisis. This study has demonstrated that, while the scientific reality of the decline is well-documented, the legal response regulating the basin remains trapped in a fragmented, ambiguous state.

Through a doctrinal and comparative analysis of domestic legislation, it is clear that national legislation among the littoral states lacks the harmonization required for transnational water management. Furthermore, existing international agreements, such as the Tehran Convention, primarily address pollution and biodiversity without providing robust mechanisms to manage the anthropogenic and natural fluctuations in water levels.

The findings of this research suggest that the environmental disaster in the region can be avoided through a new and specialized international agreement. This proposed framework must harmonize efforts through binding commitments on dam regulation and joint adaptive infrastructure. Without moving from unilateral, domestic policy to a unified, multilateral legal instrument, the socio-economic and ecological integrity of the Caspian littoral states is insufficient.

References

Alimusayev, Emin. "Analysis of Legal Challenges in Climate Regulation of Azerbaijan and Proposal for Climate Law." *Law. Human. Environment* 16, no. 4 (2025): 42–58. https://doi.org/10.31548/law/4.2025.42.

Amangeldina, Aida. "The Caspian Sea is Under Threat of Desertification: What Are the Causes and Consequences?." Central Asia Climate Information Portal, November 12, 2024. Accessed March 19, 2026. https://centralasiaclimateportal.org/publications/the-caspian-sea-is-under-threat-of-desertification-what-are-the-causes-and-consequences.

Anisimova, Aleksey, Yulia Isakova, and Olga Volkonskaya. "Trends and Prospects for the Formation of a National Model of Climate Legislation (Using the Russian Federation as an Example)." *Vniversitas Jurídica* 74 (2025). https://doi.org/10.11144/Javeriana.vj74.tpfn.

Black Sea Institute. "Aral Sea Syndrome: Why Is the Caspian Sea Shrinking?," August 21, 2024. Accessed March 19, 2026. https://blacksealaw.org/aral-sea-syndrome-why-is-the-caspian-sea-shrinking/.

Chen, Jianli, Anny Cazenave, Song-Yun Wang, and Jin Li. "Caspian Sea Level Change Observed by Satellite Altimetry." *Remote Sensing* 15, no. 3 (2023): 703. https://doi.org/10.3390/rs15030703.

Coordinating Committee on Hydrometeorology and Pollution Monitoring of the Caspian Sea (CASPCOM). *Information Bulletin on the State of the Caspian Sea Level No. 30*. 2025. http://www.caspcom.com/wp-content/uploads/2025/12/CASPCOM-Bulletin-No.30.pdf.

Coordinating Committee on Hydrometeorology and Pollution Monitoring of the Caspian Sea (CASPCOM). *Statute of the Coordinating Committee on Hydrometeorology and Pollution Monitoring of the Caspian Sea*. 2025. http://www.caspcom.com/wp-content/uploads/2025/05/Statute_CASPCOM_eng.pdf.

Court, Rebecca, et al. "Rapid Decline of Caspian Sea Level Threatens Ecosystem Integrity, Biodiversity Protection, and Human Infrastructure." *Communications Earth & Environment* 6 (2025): 261. https://doi.org/10.1038/s43247-025-02212-5.

Duisembay, Aigerim. "How the Shallowing of the Caspian Sea Affects the Economy of Coastal Regions and Logistics." Kazinform, January 7, 2026. Accessed March 19, 2026. https://www.inform.kz/ru/kak-obmelenie-kaspiya-vliyaet-na-ekonomiku-pribrezhnih-regionov-i-logistiku.

Ghahfarokhi, Mehri Shams, and Sogol Moradian. "Investigating the Causes of Lake Urmia Shrinkage: Climate Change or Anthropogenic Factors?." *Journal of Arid Land* 15, no. 4 (2023): 424–38. https://doi.org/10.1007/s40333-023-0054-z.

Ibrayev, Rashit A., Emin Özsoy, Corinna Schrum, and H.İ. Sur. "Seasonal Variability of the Caspian Sea Three-Dimensional Circulation, Sea Level and Air-Sea Interaction." *Ocean Science* 6, no. 1 (2010): 311–29. https://doi.org/10.5194/os-6-311-2010.

Kalikhan, Yerassyl. "Water Management in Kazakhstan: A Systems Approach for a Secure Future." United Nations Development Programme, March 18, 2025. Accessed March 19, 2026. https://www.undp.org/kazakhstan/blog/water-management-kazakhstan-systems-approach-secure-future.

Kayvanfar, Kamyar. "Iran's Water Crisis: Historical Roots, Ideological Dimensions and Policy Challenges." ORF Middle East, November 12, 2025. Accessed March 19, 2026. https://orfme.org/expert-speak/irans-water-crisis-historical-roots-ideological-dimensions-and-policy-challenges/.

Kepbanov, Yolbars. *Legal Protection of Climate in Turkmenistan: Assessment of the Current Situation and Development Prospects: Research Report in Sociology of Law*, 2023:4. Lund: Lund University, 2023. https://www.researchgate.net/publication/375923460.

Khalili, Ali. "Climate Changes and Iran's 7th Development Plan at a Glance." *Journal of Agricultural Meteorology* 11, no. 2 (2023): 1–3. https://doi.org/10.22125/agmj.2023.186488.

Koriche, Sifan A., Joy S. Singarayer, Hannah L. Cloke, Paul J. Valdes, Frank P. Wesselingh, Salomon B. Kroonenberg, Andrew D. Wickert, and Tamara A. Yanina. "What Are the Drivers of Caspian Sea Level Variation during the Late Quaternary?." *Quaternary Science Reviews* 283 (2022): 107457. https://doi.org/10.1016/j.quascirev.2022.107457.

Labardini, Rodrigo, and Nazrin Baghirova. *Desiccation in the Caspian Sea: On the Need to Implement Domestic and Regional Countermeasures. Analytical Policy Brief*. Baku: Institute for Development and Diplomacy, 2023. https://idd.az/media/2024/01/12/idd_policy_brief_-_labardini-baghirova_22_december.pdf?v=1.1.

Lahijani, Hamid, Suzanne A.G. Leroy, Klaus Arpe, and Jean-François Crétaux. "Caspian Sea Level Changes during Instrumental Period, Its Impact and Forecast: A Review." *Earth-Science Reviews* 241 (2023): 104428. https://doi.org/10.1016/j.earscirev.2023.104428.

Micklin, Philip. "The Aral Sea Disaster." *Annual Review of Earth and Planetary Sciences* 35 (2007): 47–72. https://doi.org/10.1146/annurev.earth.35.031306.140120.

Mislimshoeva, Bunafsha, Gulbahar Abdurasulova, Jonathan Walsh, and Jochen Statz. *Institutional Analysis of the Current National System and Processes Related to Climate Change in Turkmenistan*. International Institute for Sustainable Development, 2021. https://napglobalnetwork.org/wp-content/uploads/2021/06/napgn_en_2021_institutional-analysis-of-the-current-national-system-and-processes-related-to-climate-change-in-turkmenistan.pdf.

Mitchell, Sara M., and Neda A. Zawahri. "The Effectiveness of Treaty Design in Addressing Water Disputes." *Journal of Peace Research* 52, no. 2 (2015): 187–200. https://doi.org/10.1177/0022343314559623.

Moiseev, Timofey D., and Sofia T. Garipova. "Water Use and Ecosystem Services: A Case of Russia." *Environmental Dynamics and Global Climate Change* 13, no. 2 (2022): 60–69. https://doi.org/10.18822/edgcc105930.

Mustard, Allan, Aizhan Abilgazina, and Akbota Karibayeva. *The Silent Threat of Falling Caspian Sea Levels: A Caspian Policy Center Policy Brief*. Washington, DC: Caspian Policy Center, 2021. https://api.caspianpolicy.org/media/ckeditor_media/2021/11/04/the-silent-threat-of-falling-caspian-sea-levels.pdf.

Pietkiewicz, Michał. "Legal Status of Caspian Sea – Problem Solved?." *Marine Policy* 123 (2020): 104321. https://doi.org/10.1016/j.marpol.2020.104321.

Poberezhskaya, Marianna, and Ellie Martus. "Climate Obstruction in Russia: Surviving a Resource-Dependent Economy, an Authoritarian Regime, and a Disappearing Civil Society." In *Climate Obstruction across Europe*, edited by Robert J. Brulle, J. Timmons Roberts, and Miranda C. Spencer, 214–42. New York: Oxford University Press, 2024. https://doi.org/10.1093/oso/9780197762042.003.0009.

Safarov, Elnur, Emil Bayramov, Said Safarov, Jessica Neafie, and Alexandre Hedjazi. "Impact of Changes in the Wind Regime on the Caspian Sea Level Fluctuation and Its Relationship with SOI and NAO." *Scientific Reports* 15 (2025): 36380. https://doi.org/10.1038/s41598-025-20346-6.

Safarov, Elnur, Said Safarov, and Emil Bayramov. "Changes in the Hydrological Regime of the Volga River and Their Influence on Caspian Sea Level Fluctuations." *Water* 16, no. 12 (2024): 1744. https://doi.org/10.3390/w16121744.

Samant, Rohit, and Matthias Prange. "Climate-Driven 21st Century Caspian Sea Level Decline Estimated from CMIP6 Projections." *Communications Earth & Environment* 4, no. 1 (2023): 297. https://doi.org/10.1038/s43247-023-01017-8.

Shokri, Umud. "Caspian Sea Decline Harms Iran and Raises Regional Tensions." Stimson Center, November 7, 2025. Accessed March 19, 2026. https://www.stimson.org/2025/caspian-sea-decline-harms-iran-and-raises-regional-tensions/.

Sivakov, Dmitry O., Viacheslav V. Sevalnev, and Yuri V. Truntsevsky. "Use and Protection of Water Bodies: Corruption Cases." *E3S Web of Conferences* 203 (2020): 02016. https://doi.org/10.1051/e3sconf/202020302016.

Sopykhanova, Assel, Almkhan Maytanov, Alla Kiseleva, and Roza Zhamiyeva. "Problems of Legal Regulation and State Policy Measures Related to Nature Management in the Framework of Achieving the SDGs: Examples from Russia and Kazakhstan." *Sustainability* 15, no. 2 (2023): 1042. https://doi.org/10.3390/su15021042.

State News Agency of Turkmenistan. "Presentation of the Draft Law 'On Climate Change' Was Held in Ashgabat." Turkmenistan: Golden Age, June 6, 2024. Accessed March 19, 2026. https://aarhusashgabat.org/blog/v-ashhabade-sostoyalas-prezentacziya-zakonoproekta-ob-izmenenii-klimata/.

Uchet.kz. "New Water Code Entered into Force." June 10, 2025. Accessed March 19, 2026. https://uchet.kz/news/novyy-vodnyy-kodeks-vstupil-v-silu/.

United Nations Economic Commission for Europe. *Progress on Transboundary Water Cooperation under the Water Convention: Third Report on Implementation*. 2024. https://unece.org/sites/default/files/2024-12/2417627_E_PDF_WEB.pdf.

United Nations Environment Programme. "Caspian Sea Fluctuations and Climate Change." Working Paper, UNEP DHI Partnership, Nairobi, 2024. https://unepdhi.org/wp-content/uploads/sites/2/2024/11/Caspian_Sea_working_paper.pdf.

Venitsianov, Yevgeniy V. "Modern Problems of Water Protection in Russia." *IOP Conference Series: Earth and Environmental Science* 321 (2019): 012033. https://doi.org/10.1088/1755-1315/321/1/012033.

Voynova, Maria V. "Main Stages of Developing Environmental Legislation of Islamic Republic of Iran on Environmental Protection of Caspian Sea." *Oil and Gas Technologies and Environmental Safety* 2 (2023): 69–82. https://doi.org/10.24143/1812-9498-2023-2-69-82.

Zhavoronkova, Natalia G., and Vyacheslav B. Agafonov. "The Role of National Climate Law in Ensuring the 'Energy Transition'." *Lex Russica* 17, no. 2 (2022): 151–62. https://doi.org/10.17803/1994-1471.2022.135.2.151-162.

Ziganshina, Dinara R. "Institutional Mechanisms for Preventing and Resolving Cross-Border Water Disputes." *AJIL Unbound* 115 (2021): 195–200. https://doi.org/10.1017/aju.2021.20.

Review of European and Comparative Law | **2026**
Vol. 64, No. 1, 213–216
https://doi.org/10.31743/recl.19614
Received: 25 January 2026 | Accepted: 22 February 2026 | Published: 31 March 2026

Stevan Lilić, *Administrative Law in Serbia*, Belgrade: Faculty of Law, University of Belgrade, 2022, pp. 383

Marko Milenković
PhD, LLM, Principal Research Fellow, Institute of Social Sciences, Belgrade, Republic of Serbia; e-mail: mmilenkovic@idn.org.rs
https://orcid.org/0000-0001-9170-1571

The book *Administrative Law in Serbia*, by Professor Stevan Lilić, one of the leading academics in administrative law in the Western Balkans region, provides a comprehensive and systematic contemporary account of Serbian administrative law, available in English. Professor Stevan Lilić's academic career spans 40 years, teaching Administrative Law, Public Administration and Environmental Law at the University of Belgrade and the UDG University in Montenegro, and working with many other universities as a research fellow, visiting professor and guest lecturer. This book adds to the list of over 400 publications and provides the most comprehensive account of the topic, both for the academic and wider professional audience.

Administrative Law in Serbia offers a systematic doctrinal examination of the conceptual foundations, institutional organization, sources, procedures, and judicial oversight of administration in Serbia, while carefully placing these developments within the broader context of the European Administrative Space and Serbia's EU accession process. While Serbian administrative law has been the subject of various monographs, commentaries, and textbooks in the native Serbian language, few works have attempted to systematize the field for an international audience. Professor Lilić's monograph is valuable not only as an authoritative overview of the national system, but also as a reference point for scholars who wish to view Serbian administrative developments within the broader context of European public law trends. As such, the volume successfully functions both as an advanced university textbook and as a reliable reference work for scholars and practitioners engaged in comparative administrative law and European integration.

The monograph is structured into seven coherent and conceptually well-balanced sections. The opening part of the book provides a broad theoretical and historical foundation for understanding administration as both an institution and a legal concept. The author revisits classical approaches to the administrative state, systems theory, and socio-technological accounts of governance in order to illustrate the shifting boundaries of administrative authority in modern states. His discussion of administration as an instrument of public service, as opposed to a mere extension of a coercive executive function, aligns with the dominant European understanding, which emphasizes legality, accountability, and the protection of individual rights. The historical development of administration in Serbia is described with clarity. Professor Lilić traces the emergence of modern Serbian administration from the nineteenth century to the present, highlighting periods of institutional consolidation, episodes of politicization, and the gradual

ISSN 2545-384X (Online)

adoption of European administrative principles. For international readers, this is a useful contextualization of Serbian public administration within the broader evolution of post-socialist administrative reforms. The book effectively outlines the primary shifts in doctrine and institutional design that underpin the current structure of the administrative system in Serbia.

More specifically, chapter I (pp. 17–72) develops a dense theoretical framework for understanding administration, combining classical legal doctrine with systems theory and socio-technological approaches. The author revisits the distinction between administration as an exercise of authority and administration as a public service, engaging with concepts such as legality, legitimacy, and the rule of law, while contextualizing Serbian administrative doctrine within broader European intellectual traditions (pp. 25–39). This chapter is not merely introductory: it establishes the conceptual vocabulary that structures the rest of the monograph, particularly the author's consistent distinction between political decision-making and administrative implementation. This theoretical orientation of the monograph is explicitly grounded in the general systems theory, which the author studied in his previous works. Professor Lilić says:

> The modern theoretical notion of administration as a system for social regulation is based on the results of the general theory system and the systems methodology in determining complex natural and, especially, social phenomena, adding that the general system approach is an indispensable theoretical setting for the contemporary study of complex social systems, especially administrative systems (pp. 34–35).

In the parts devoted to administrative law as positive law and as a scholarly discipline, Professor Lilić presents the conceptual architecture of Serbian administrative law. The author examines its subject matter, internal structure, and relationship to constitutional law, public policy, and administrative sciences. The distinction between administrative law as a regulatory framework governing administrative action and administrative law as an academic field is demonstrated with precision.

Chapters II and III (pp. 75–187) move from theory to doctrinal systematization. Here, the author offers a detailed account of administrative law as positive law, addressing its subject matter, sources, and internal differentiation between general and special administrative law. This discussion is complemented by an extensive historical overview of the development of administrative law as a scientific discipline in Serbia and the former Yugoslavia (pp. 108–121). Particularly valuable for comparative scholars is the treatment of sources of administrative law, which maps constitutional norms, statutory law, subordinate legislation, and case law in a way enabling direct comparison with continental European administrative systems (pp. 133–148).

A significant contribution made by the book is its clear articulation of the sources of Serbian administrative law, including constitutional provisions, statutory law, subordinate regulations, and principles derived from case law. In doing so, the author provides a framework that is easily comparable to those used in other European jurisdictions. The inclusion of European administrative principles, such as legality, proportionality, legitimate expectations, and the right to be heard signals the increasingly hybrid nature

of administrative regulation in accession countries. While the book is not primarily concerned with the influence of EU administrative law or the European Administrative Space on Serbian law, it consistently notes areas of convergence, particularly in procedural guarantees and judicial oversight.

The book's treatment of administrative organization is factual, systematic, and aligned with the internal logic of Serbian public administration law. The author describes the structure of state administration, provincial and local bodies, public agencies, inspectorates, and regulatory authorities. The exposition is both descriptive and analytical, providing sufficient detail for international readers who may be unfamiliar with the institutional layout.

The discussion of civil service and the legal status of public employees is concise but effective. Normative elements, such as recruitment, rights and obligations, and disciplinary procedures, are linked to broader administrative ethics and professional responsibility. This section underscores a recurring theme in the book: the expectation that administrative bodies act in a manner consistent with public trust and democratic accountability. As noted by the author

> A public servant, as an authorized representative of the state, realizes the public interest by performing his/her duties and functions that are manifested in administrative action. Public interest or public good is therefore closely related to administrative decisions, because it gives them direction and meaning in everything they do (pp. 180–181).

One of the particularly valuable strengths of the book is the structured presentation of control mechanisms over administrative authorities. In chapter IV (pp. 191–213), Professor Lilić provides a systematic overview of control mechanisms over administrative action, distinguishing between political, administrative, judicial, and constitutional forms of oversight. The analysis clarifies the respective roles of internal administrative supervision, judicial review before the Administrative Court, and constitutional complaint mechanisms, highlighting their complementary functions in securing legality and protecting individual rights (pp. 202–208). The author identifies political, administrative, and judicial forms of control and outlines their respective competences and limitations. The chapters on oversight provide a clear, normative map of accountability structures in Serbia, including the roles of various institutions. The author's treatment of control mechanisms is consistent with European doctrinal approaches, particularly in jurisdictions that emphasize multi-layered oversight rather than hierarchical control alone. For researchers unfamiliar with the Serbian model, this section provides a reliable overview of institutions through which legality and procedural fairness are enforced.

Chapter V (pp. 217–318) constitutes the core of the monograph and reflects the author's long-standing scholarly engagement with administrative procedure. In more than one hundred pages, Lilić offers a meticulous analysis of the 2016 Law on General Administrative Procedure (LGAP), including its principles, procedural stages, and newly introduced legal instruments, such as administrative contracts, guarantee acts, and the concept of a single administrative "point of contact" (pp. 240–275). The author does not merely describe these innovations, but critically examines their conceptual coherence,

notably questioning the statutory definition of "administrative procedure" itself and the internal consistency of the law's basic concepts (pp. 242–247). Here, Professor Lilić demonstrates his long-standing dedication to the field and study of the procedural developments in the post-Yugoslav area. Of particular value is the analytical treatment of ambiguities in the new LGAP. The author presents these issues with doctrinal precision, avoiding both overstatement and unnecessary criticism. This contributes to the book's reliability as a reference work. In a European context, the chapters on procedure offer an instructive example of how accession states adapt their administrative procedural laws to align with principles derived from EU law and Council of Europe standards, but often in a complex setting of institutional and legal reforms.

Chapter VI (pp. 321–348) addresses administrative disputes and judicial protection against administrative action. The author examines jurisdictional rules, standing, procedural requirements, and the legal effects of judgments, while drawing attention to structural shortcomings of the Serbian model. As with previous sections, the exposition is doctrinal and faithful to the text of the law. One important observation concerns the absence of appeal as a regular legal remedy within the Law on Administrative Disputes, an issue noted in international reports on legal developments in the country. As the author himself notes, this configuration results in a "characteristic anomaly," given that the Constitution guarantees the right to appeal against decisions affecting individual rights, which explains why "the European Commission's annual Serbia Progress Reports continuously state that the legal framework for legal protection in administrative disputes is not in accordance with European standards" (p. 343). The discussion also touches on the role of the Constitutional Court and the relationship between constitutional review and administrative justice. For comparative scholars, these sections provide insight into how judicial review structures in Serbia relate to European models that emphasize effective legal protection.

The final section (chapter VII) examines the place of Serbian administrative law within the context of EU accession, outlining key reform priorities and the broader trajectory of administrative convergence. The discussion offers a useful overview of the institutional and legislative changes necessary to meet EU expectations in public administration reform. The book's orientation toward European standards is one of its core strengths. Even when European influences are not explicitly analyzed, they form a consistent backdrop to the doctrinal exposition. This makes the monograph highly relevant for comparative administrative law and for scholars assessing the legal dimensions of EU enlargement.

In conclusion, *Administrative Law in Serbia* by Professor Stevan Lilić is a theoretically coherent and methodologically structured monograph with an in-depth overview of the complex area of administrative law in Serbia. Its doctrinal contribution is a clear and accessible presentation of administrative law in Serbia – a valuable resource for international scholars, legal practitioners, and foreign students. For readers interested in comparative administrative law, Professor Lilić's outstanding monograph provides an indispensable mapping of Serbian administrative norms and institutions, contextualizing them, sometimes explicitly and sometimes implicitly, within the broader European administrative tradition.