Aleksandra Nikolova Marković*
https://orcid.org/0009-0000-9724-8739
Borivoje Baltezarević**
https://orcid.org/0000-0002-6798-6981

UDC: 005.334:334.72

DOI: 10.5937/MegRev2503121N
Review scientific paper
Received 20.08.2025.
Approved: 23.12.2025.

CORPORATE SECURITY AND CORPORATE LAW: LEGAL DUTIES OF COMPANIES IN PROTECTING DATA AND INFORMATION

Abstract: *The increased digitalization of business activities has significantly exposed companies to data and information abuse risks, making their protection a central matter in corporate security. This paper examines the relationship between corporate security and corporate law, focusing on the legal obligations of organizations in protecting data and information. In the first part of the paper, the corporate security in the digital environment is analyzed, highlighting the increased risks for abuse of the digital data and information. Furthermore, the paper examines the role of corporate law in defining the duties of the board of directors in data and information protection and their liability in case of cyber incidents. The paper also examines data and information protection as a corporate law obligation by highlighting how corporate law provides a framework for the implementation of data protection and cybersecurity laws within organizations. The paper concludes that adequate protection of data and information can be achieved only with the integration of corporate security measures into corporate governance structures and that acknowledging data and information protection as a corporate law obligation is essential for creating lawful and resilient corporate security systems in a rapidly changing digital environment.*

Keywords: *corporate security, corporate law, data and information protection, directors' duties*

* Faculty of Law, Megatrend University, Belgrade, Republic of Serbia.
E-mail: anikmarkovic@gmail.com
** Institut za srpsku kulturu Priština-Leposavić, Republic of Serbia.
E-mail: baltezb@yahoo.co.uk

INTRODUCTION

The increased use of informational technologies in executing business activities has contributed to changing the nature of the assets on which companies build their businesses. Traditional tangible assets are increasingly losing their significance in terms of the value they have for the company, while intangible assets, which include data and information, are taking precedence when it comes to assets of greatest importance to the company. In this sense, companies' data and information have become a central asset that contributes to the value of the organization and its efficiency. The synergy between semiotics and AI is inextricable when delving into digital culture.[1]

Data and information have great value for companies because, with their proper use, they can obtain significant information about market trends, customer habits and needs, about choosing the right pricing strategy, and for developing a business strategy based on real data analysis. Furthermore, the protection of business data and information, in the era of developed information technologies and frequent cyber attacks, takes a primary place in corporate security, because any data breach or misuse can lead to serious damage to the company's reputation, as well as to the privacy of customers who have trusted the organization to store and handle their data.[2]

In the context of corporate security and the protection the organization's information and data, corporate law plays a very important role. In modern organizations, corporate security is no longer perceived merely as a technical function, but as a component of a broader organizational and legal arrangement, in which legal rules defining the obligations and responsibilities of the company and its management bodies establish standards for the formation and functioning of corporate governance systems. Corporate law, in addition to determining the manner of organization in a company and determining the competencies of the bodies in the company, is also important for managing potential risks, including risks related to the protection of information and data. According to the postulates of corporate law, the management bodies must act with a duty of care and in the best interest of the organization. Inadequate fulfillment of these duties may result in liability of the management bodies for the damage caused.[3] Corporate law, through its principles and regulatory norms, establishes the basis for incorporating information

1 Borivoje, B. (2023): "Decoding identity and representation in the age of AI", *MEGATREND REVIJA*, *20*(2), 141–146, 143.

2 Kamiya, S., Kang, J. K., Kim, J., Milidonis, A. & Stulz, R. M. (2018): "What is the impact of successful cyberattacks on target firms?", National Bureau of Economic Research, 24409.

3 Gale, M. (2022): "Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead", *Computers & Security*, *121*, 102840.

security and cybersecurity into corporate strategy and governance, highlighting responsible information management as a fundamental condition for corporate stability and sustainability.

The aim of this paper is to analyze the relationship between corporate security and corporate law, focusing on the legal duties of companies to protect data and information. In addition, the paper adopts a comparative law perspective, examining how the EU legal system, conceptualizes corporate duties regarding the safety of data and information.

1. CORPORATE SECURITY IN THE DIGITAL ENVIRONMENT

In the last two decades, the presence of individuals, companies, and various types of organizations in cyberspace has been continuously increasing. When it comes to business organizations, in modern society, there is almost no business operation that is carried out manually, without the presence of digital technologies. The dependence on digital technologies has brought many positive effects in terms of the rapid exchange of information and the efficiency of business processes, but it has also largely opened up space for cyber threats and attacks.[4] Research conducted by Microsoft and many other analytical companies regarding cyber threats and attacks has come to the conclusion that companies and individual users of digital technologies are exposed to cyber attacks like never before.[5] According to the 2016 Internet Security Report, cyber-attacks exposed over half a billion data records, and this figure has shown a continuous upward trend in subsequent years.[6] The widespread use of information technologies has resulted in an increased number of abuses and technologically advanced and adaptive methods of action in cyber attacks. The increased abuse of information systems requires the existence of a system that aims to protect the information, data, and reputation of the company. Historically, corporate security has always been about protecting a company's tangible assets, as well as trade secrets. The rapid development of IT technologies has contributed to expanding the scope, and in modern society, corporate security is also associated with the protection of intangible assets, such as digital information, data, algorithms, legal regulations, etc. In addition, corporate security in modern times is perceived as a broad system, interconnected, consisting of governance

4 Baltezarević, I. & Baltezarević, R. (2021): "Sajber bezbednost: Izgradnja digitalnog poverenja", *Megatrend Revija*, *18*(4), 269–280.

5 Kaurin, T. & Skakavac, Z. (2018): "Corporate security in the cyber environment", 151–172, in: Trivan, D. (ed.), *Contemporary concept of corporate security*.

6 Symantec (2017): *Internet security threat report*, Volume 22, https://www.symantec.com/en/ca/security-center/threat-report.

arrangements, internal policies, and technical and human measures aimed at ensuring the protection of a company's physical, digital, intellectual, and human assets against threats originating from both within and outside the organization.[7]

In a broader sense, corporate security refers to both cybersecurity and to:[8]

- Protection of information infrastructure – including protection of all kinds of information, not only digital information,
- Security of the network in the inner organization and the network between the clients and the organization,
- Internet services protection, which is connected with the availability of internet services in the organization.

As a result of the rapid change of the digital landscape, corporate security has changed its form from just an operational matter to a significant strategic issue.[9] From a legal perspective, corporate security refers to the company's obligations to act responsibly, within the framework of the law, and without knowingly causing harm to third parties. Given that digital technologies have become a central tool in the performance of business operations, their misuse can seriously jeopardize the continuity of business activities, and to violate customer trust. As a result of such misuse, failure of corporate security could also occur. In this sense, corporate security must be perceived from a multidimensional perspective as an area that encompasses legal regulation, governance processes, and the security of the company's assets.

2. CORPORATE LAW, THE LEGAL DUTIES OF COMPANIES, AND THE ROLE OF THE BOARD OF DIRECTORS REGARDING DATA AND INFORMATION PROTECTION

The fundamental elements of the corporate law framework are the duties of the companies and their managing bodies to act with due care, loyalty, in informed basis and in a good faith.[10] These duties shape the way an organization is structured, controlled and overseen. Corporate law does not explicitly provide legal norms relating to data protection and corporate security, but it provides clear rules that every organization should apply to organize its activities and resources in order

7 Stanojević, M. (2025): "Corporate security and protection of company reputation in crisis situations", *Megatrend Review*, *22*(1), 161–179.

8 Sutton, D. (2017): *Cyber security: A practitioner's guide*, BCS, The Chartered Institute for IT.

9 Stanojević, M. (2025): "The role of information technologies in modern corporate security", *Megatrend Revija*, *22*(1), 231-242.

10 OECD (2015): *G20/OECD Principles of Corporate Governance*, OECD Publishing, Paris.

to recognize potential risks, perform smooth operations, and ensure that every employee knows their responsibilities and duties. This includes the establishment of internal control mechanisms, reporting systems, and compliance frameworks that are adequate to the company's activities and risk profile.[11]

In the modern digital environment, misuse of data and information can have multifaceted consequences for the company and for the stakeholders. The failure to adequately store and manage the data and information risks may result with a breach of corporate law duties.[12] This breach of duty can be avoided if companies comply with the norms of corporate law, which indirectly grants companies the right to determine how data and information should be protected. However, in the case of non-compliance or in case of incidents, liability is provided for corporate governance bodies when reasonable and proportionate measures are not taken.

Boards of directors play a central role in shaping corporate security policies. They are responsible for setting strategic priorities, oversight, and ensuring that in the security of data and information processes, all measures to ensure protection are taken conscientiously.[13] An inadequate corporate governance system, which can be seen in unclearly defined and delegated responsibilities among employees, unclear and insufficient mechanisms for oversight and reporting of potential risks, often leads to failures in data and information protection.

From a historical perspective, the role of boards in relation to cybersecurity and the protection of data and information was relatively limited. Just over a decade ago, board members were generally not expected to possess detailed knowledge of cybersecurity measures or technical safeguards. However, the growing frequency and severity of cyber threats have fundamentally changed this position. In modern corporate practice, digital protection of data and information can no longer be treated as a purely technical issue. Instead, boards are increasingly required to engage with the matter of proper protection of data and information in order to ensure the security and continuity of business operations.

Corporate law supports this change through fiduciary duties imposed on directors, particularly the duties of due care and oversight. The duty of due care requires directors to make decisions on an informed basis and with appropriate diligence, while the duty of oversight obliges them to monitor the company's operations. These duties are of particular importance in the context of protecting data and information, as they require directors to ensure that proper systems for identifying, assessing, and managing cyber risks are in place.

11 Bainbridge, S. M. (2002): "The board of directors as nexus of contracts", *Iowa Law Review*, *88*, 1–34.

12 Rothrock, R. A., Kaplan, J. & van der Oord, F. (2018): "The board's role in managing cybersecurity risks", *MIT Sloan Management Review*, *59*(2), 12–15.

13 OECD (2015): *G20/OECD Principles of Corporate Governance*, OECD Publishing, Paris.

Importantly, corporate law does not require directors to possess technical expertise or to implement protective measures personally. Rather, it grants them the authority and responsibility to establish organizational structures that minimize cyber risks. This includes ensuring the timely flow of information, which can enable an informed decision-making process. As emphasized in the academic literature, directors' duties focus primarily on decision-making processes and the quality of information available within the organization.[14] In similar way, Payne observes that cyber threats constitute a modern risk that clearly falls within directors' oversight responsibilities.[15] From a corporate law perspective, governance failures related to data protection may signal a breach of the duty to organize and supervise the company in a responsible way.

3. DATA AND INFORMATION PROTECTION AS A CORPORATE LAW OBLIGATION

As discussed before, corporate law has a very important role in ensuring the protection of data and information in the digital environment. Corporate law serves as a framework that regulates the way in which data protection laws should be implemented in corporate governance. These frameworks define the conditions under which companies may collect, store, process, and disclose personal information, while also obliging them to adopt appropriate safeguards mechanisms against unauthorized access and data breaches.[16]

An essential element of corporate law in the protection of the data and information area is the possibility for the application of enforcement mechanisms and the imposition of fines for abuse and non-compliance. The implementation of significant fines serves as an effective deterrent, as it links non-compliance with data protection rules to concrete consequences. Through these mechanisms, data protection obligations become mandatory, ensuring that companies treat the protection of personal data as a core responsibility.[17]

Last, but not least aspect of the corporate law in the protection of data and information is that Corporate Law offers legal regulation in cases of data breaches

[14] Hill, J. G. & Conaglen, M. (2018): *Directors' duties and corporate governance*, Oxford University Press.

[15] Payne, A. M. (2019): "What the Hack?! Reexamining the Duty of Oversight in an Age of Cybersecurity", *Georgia Law Review*, *54*, 1–59.

[16] Miller & Associates (2023): "Data privacy and corporate law: Protecting information in a digital world", Expert Law Firm, https://www.expertlawfirm.com/data-privacy-and-corporate-law-protecting-information-in-a-digital-world/.

[17] Ibid.

and damage caused. Companies are expected to take reasonable measures to protect not only their own information, but also data entrusted to them by customers, employees, and business partners. This means that companies, or rather the board of directors, in accordance with the principles of corporate law, should act with due care, but in the event of an incident, if it is shown that the management body did not act with due care, it may be held liable for the damage caused. Contemporary legal discussions recognize that data breaches and cyber incidents are frequently the result of internal organizational failures, including inadequate governance arrangements, insufficient oversight by corporate bodies, and weaknesses in risk management practices.[18]

4. COMPARATIVE LAW PERSPECTIVE: EUROPEAN UNION

In the European Union, the protection of data and information as corporate security obligations is structured as a combination of corporate law principles and regulatory frameworks, such as the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS Directive). The EU corporate law remains at the level of general principles, but it highlights the responsibility of companies to ensure that their operations are undertaken in a lawful manner and with due care. The GDPR[19] strengthens this concept by imposing strict obligations on companies to protect personal data, supported by significant administrative fines. The General Data Protection Regulation provides very rigorous rules for organizations on the collection, processing, and storage of personal data. GDPR applies to every organization inside the EU or outside the EU that handles the personal data of EU citizens. Fines can reach up to €20 million or 4% of the organization's annual global turnover, whichever is greater.[20] GDPR has exposed businesses with high compliance costs,[21] but its implementation is very important in the contemporary digital environment. Importantly, GDPR compliance is treated as an organizational responsibility requiring appropriate activities

18 Sutton, D. (2017): *Cyber security: A practitioner's guide*, BCS, The Chartered Institute for IT.

19 European Union (2016): "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 (General Data Protection Regulation)", *Official Journal of the European Union*, *L119*, 1–88.

20 Nikolova Marković, A., Lutovac, N. & Milović, M. (2025): *Legal challenges in the evolving cybersecurity landscape: National and international perspectives*, Megatrend University, https://megatrend.edu.rs.

21 Smirnova, Y. & Travieso-Morales, V. (2024): "Understanding challenges of GDPR implementation in business enterprises: A systematic literature review", *International Journal of Law and Management*, *66*(3), 326–344.

from the companies. Therefore, corporate governance plays an important role in ensuring compliance and maintaining corporate security. The NIS Directive[22] was adopted by the European Union in 2016 and later amended with NIS2[23] in 2022. This NIS Directive is the first EU document related to cybersecurity, with the main aim of protecting the critical infrastructure of organizations.[24] Obligations of the member states are: ensuring a high level of network and information security through establishing national strategies, competent authorities, and incident reporting obligations for operators and digital service providers.[25] From a corporate law aspect, the EU system of data protection incorporates data protection into the concept of corporate liability.

CONCLUSION

This paper has argued that corporate security and corporate law are inextricably linked in the area of protection of data and information. Failures to protect data and information can result in significant legal and reputational consequences for companies. These include regulatory investigations, civil liability, fines, and reputational damage. Therefore, the protection of data and information in contemporary organizations should be considered as a legal duty supported by corporate law principles. The analysis of the GDPR and the NIS regulatory framework has shown how EU data protection and cybersecurity regulations shape corporate governance obligations and influence the interpretation of corporate law duties, particularly the duties of care and oversight.

The main role of corporate law in protecting data and information in a digital environment is to offer a legal infrastructure through which data protection laws should be implemented in the corporate governance bodies. By highlighting liability, oversight, clear division of the roles, and risk management, corporate law

22 European Union (2016): "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)", *Official Journal of the European Union*, *L194*, 1–30.

23 European Union (2022): "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)", *Official Journal of the European Union*, *L333*, 80–152.

24 Nikolova Marković, A., Lutovac, N. & Milović, M. (2025): *Legal challenges in the evolving cybersecurity landscape: National and international perspectives*, Megatrend University, https://megatrend.edu.rs.

25 Markopoulou, D., Papakonstantinou, V. & de Hert, P. (2019): "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation", *Computer Law & Security Review*, *35*(6), 1-11.

transforms data and information protection into a central element of corporate security. In an era of rapidly changing digital environment and increasing cyber threats, recognizing the relationship between corporate security and corporate law in protecting information and data is essential for maintaining sustainable corporate operations.

LITERATURE

- Baltezarević, I. & Baltezarević, R. (2021): "Sajber bezbednost: Izgradnja digitalnog poverenja", *Megatrend Revija*, *18*(4), 269–280.
- Borivoje, B. (2023): "Decoding identity and representation in the age of AI", *MEGATREND REVIJA*, *20*(2), 141–146, 143.
- European Union (2016): "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)", *Official Journal of the European Union*, *L194*, 1–30.
- European Union (2016): "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data (General Data Protection Regulation)", *Official Journal of the European Union*, *L119*, 1–88.
- European Union (2022): "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cyber security across the Union (NIS 2 Directive)", *Official Journal of the European Union*, *L333*, 80–152.
- Gale, M. (2022): "Governing cyber security from the boardroom: Challenges, drivers, and ways ahead", *Computers & Security*, *121*, 102840.
- Hill, J. G. & Conaglen, M. (2018): *Directors' duties and corporate governance*, Oxford University Press.
- Kamiya, S., Kang, J. K., Kim, J., Milidonis, A. & Stulz, R. M. (2018): "What is the impact of successful cyber-attacks on target firms?", National Bureau of Economic Research, 24409.
- Markopoulou, D., Papakonstantinou, V. & de Hert, P. (2019): "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation", *Computer Law & Security Review*, *35*(6), 1-11.
- Miller & Associates (2023): "Data privacy and corporate law: Protecting information in a digital world", Expert Law Firm, https://www.expertlawfirm.com/data-privacy-and-corporate-law-protecting-information-in-a-digital-world/.

- Nikolova Marković, A., Lutovac, N. & Milović, M. (2025): *Legal challenges in the evolving cybersecurity landscape: National and international perspectives*, Megatrend University, https://megatrend.edu.rs.
- OECD (2015): *G20/OECD Principles of Corporate Governance*, OECD Publishing, Paris.
- Payne, A. M. (2019): "What the Hack?! Reexamining the Duty of Oversight in an Age of Cybersecurity", *Georgia Law Review*, *54*, 1–59.
- Rothrock, R. A., Kaplan, J. & van der Oord, F. (2018): "The board's role in managing cybersecurity risks", *MIT Sloan Management Review*, *59*(2), 12–15.
- Smirnova, Y. & Travieso-Morales, V. (2024): "Understanding challenges of GDPR implementation in business enterprises: A systematic literature review", *International Journal of Law and Management*, *66*(3), 326–344.
- Stanojević, M. (2025): "Corporate security and protection of company reputation in crisis situations", *Megatrend Revija*, *22*(1), 161–179.
- Stanojević, M. (2025): "The role of information technologies in modern corporate security", *Megatrend Revija*, *22*(1), 231-242.
- Sutton, D. (2017): *Cyber security: A practitioner's guide*, BCS, The Chartered Institute for IT.

Aleksandra Nikolova Marković
Borivoje Baltezarević

Pregledni naučni rad
Primljen 20.08.2025.
Odobren 23.12.2025.

KORPORATIVNA BEZBEDNOST I POSLOVNO PRAVO: PRAVNE OBAVEZE PRIVREDNIH DRUŠTAVA U ZAŠTITI PODATAKA I INFORMACIJA

Apstrakt: *Povećana digitalizacija poslovnih aktivnosti značajno je izložila privredna društva rizicima zloupotrebe podataka i informacija, čineći njihovu zaštitu centralnim pitanjem korporativne bezbednosti. Ovaj rad razmatra odnos između korporativne bezbednosti i poslovnog prava, sa posebnim osvrtom na pravne obaveze privrednih subjekata u pogledu zaštite podataka i informacija. U prvom delu rada analizira se korporativna bezbednost u digitalnom okruženju, uz ukazivanje na povećane rizike zloupotrebe digitalnih podataka i informacija. Nadalje, rad ispituje ulogu poslovnog prava u definisanju dužnosti upravnog odbora u oblasti zaštite podataka i informacija, kao i njihovu odgovornost u slučaju sajber incidenata. Rad takođe razmatra zaštitu podataka i informacija kao obavezu koja proizilazi iz poslovnog prava, naglašavajući da poslovno pravo obezbeđuje normativnu infrastrukturu za primenu propisa o zaštiti podataka i sajber bezbednosti unutar privrednih društava. U zaključku se ističe da se adekvatna zaštita podataka i informacija može ostvariti isključivo integracijom mera korporativne bezbednosti u strukture korporativnog upravljanja, te da je priznavanje zaštite podataka i informacija kao obaveze koja proističe iz poslovnog prava od suštinskog značaja za uspostavljanje zakonitih i otpornih sistema korporativne bezbednosti u uslovima dinamičnog digitalnog okruženja.*

Ključne reči: *korporativna bezbednost, poslovno pravo, zaštita podataka i informacija, dužnosti direktora*