Legal Issues in the Digital Age. 2023. Vol. 4. No. 2.
Вопросы права в цифровую эпоху. 2023. Том 4. № 2.

*Research article*
УДК: 342
DOI:10.17323/2713-2749.2023.2.78.121

# Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age

**Naeem Allahrakha**

Tashkent State University of Law, 35 uy, Sayil ko ‘ch, Toshkent 100047 sh., Uzbekistan,

Chauharynaeem133@gmail.com, 0000-0003-3001-1575

**Abstract**

In today’s digital world the need to maintain cyber-security and protect sensitive information is more important than ever. However, this must be balanced against the right to privacy, which is also a fundamental human right. This article provides an overview of the legal and ethical considerations involved in balancing cyber-security and privacy in the digital age. It explores the challenges of implementing effective cyber-security measures while respecting privacy rights, and discusses the current legal framework for cyber-security and privacy in various jurisdictions. The article also considers the ethical implications of balancing these two important values and suggests ways in which cyber-security and privacy concerns can be reconciled in a general context. By highlighting the importance of a careful balance between cyber-security and privacy, this article aims to raise awareness of the need for ethical and legal considerations in the development of digital technologies and their regulation.

**Keywords**

cyber-security; privacy; digital age; legal considerations; ethical considerations.

***For citation***: Allahrakha N. (2023) Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age. *Legal Issues in the Digital Age*, vol. 4, no. 2, pp. 78–121. DOI:10.17323/2713-2749.2023.2.78.121

## 1. Introduction

In the contemporary world with the exponential growth of digital technologies, the need to maintain cyber-security and protect sensitive information is more crucial than ever. However, this must be balanced against the right to privacy, which is also a fundamental human right. The issue of balancing cyber-security and privacy is a complex one that requires careful consideration of legal and ethical implications. [Singer P., Tushman M., 2021]. The article explores the topic in detail, examining challenges of implementing effective cyber-security measures while respecting privacy rights, current legal framework for cyber-security and privacy in various jurisdictions, and ethical implications of balancing these two values. The aim of article is to raise awareness of the need for ethical and legal considerations in the development of digital technologies and their regulation. The introduction provides an overview of the article and highlights its significance in context of digital age.

### 1.1. Background

The advancement of digital technologies has revolutionized the way we live, work, and communicates. The widespread use of the Internet and digital devices has made our lives easier, but it has also created new challenges, particularly in the area of cyber-security and privacy. With the increasing amount of personal and sensitive information being stored online, protecting this information from cyber-attacks has become a critical concern for individuals, businesses, and governments. At the same time, the right to privacy is also a fundamental human right recognized by international law. Protecting individuals' privacy rights in the digital age has become a challenging task, as the collection and processing of personal data have become more widespread.

Balancing the need for reasonable cyber-security measures and privacy rights has become a critical challenge for policymakers, businesses, and individuals alike. This background highlights the importance of examining the legal and ethical considerations involved in balancing cyber-security and privacy in the digital age. Understanding the challenges and implications of this balance can provide insights into the development of effective cyber-security policies that respect privacy rights [Kshetri N., 2021].

### 1.2. Research Problem

The issue of balancing cyber-security and privacy in the digital age presents a significant challenge for policymakers, businesses, and individuals. While cyber-security is critical in protecting sensitive information from cyber-attacks, the collection and processing of personal data raises concerns about the violation of privacy rights. The challenge is to find a balance between cyber-security and privacy that allows for the protection of sensitive information without compromising individual privacy rights. This article seeks to address the research problem of how to balance cyber-security and privacy in the digital age. The article examines the legal and ethical considerations involved in this balance, explores the challenges of implementing effective cyber-security measures while respecting privacy rights, and discusses the current legal framework for cyber-security and privacy in various jurisdictions. By doing so, the article aims to provide insights into how to reconcile cyber-security and privacy concerns in a general context.

### 1.3. Objective of Research

The objectives of the author are to provide an overview of legal and ethical considerations involved in balancing cyber-security and privacy in the digital age, and to explore the challenges of implementing effective cyber-security measures while respecting privacy rights. The article aims to discuss the current legal framework for cyber-security and privacy in various jurisdictions and to consider the ethical implications of balancing these two important values. The article suggests ways in which cyber-security and privacy concerns can be reconciled in a general context, highlighting the importance of a balance between cyber-security and privacy. Ultimately, the objective of the article is to raise awareness of the need for ethical and legal considerations in the development of digital technologies and their regulation.

### 1.4. Literature

In recent years a growing number of scholars have explored the ethical and legal implications of balancing cyber-security and privacy in the digital age. For instance, the traditional dichotomy between security and privacy is a false one, and that the two are mutually reinforcing concepts that should be balanced together. Privacy is not just an individual right, but

also serves important social and democratic functions, such as protecting free speech and limiting government overreach [Pavlou P., Lewis K., 2020].

Similarly, scholars like Greenwald have highlighted the dangers of government surveillance and data collection, arguing that these practices can undermine individual privacy rights and erode trust in democratic institutions. Greenwald, for instance, exposed the extent of U.S. government surveillance activities through his reporting on the Edward Snowden leaks, revealing how the government collected vast amounts of data on private citizens without their knowledge or consent [Greenwald G., 2021: 78–86]. Other scholars have focused on the challenges of implementing effective cyber-security measures while respecting privacy rights. For example, Yoo [Yoo C., 2015: 129–137] argues that privacy protections can actually enhance cyber-security by reducing the risks of data breaches and identity theft. However, he also notes that overly strict privacy laws can inhibit law enforcement and national security agencies from accessing important data and preventing terrorist attacks. In addition to these legal and ethical considerations, scholars have also explored the economic implications of cyber-security and privacy. Among others,some people [Acquisti A., Grossklags, 2013: 1–32] argue that privacy as a valuable commodity can be traded in the marketplace, and that individuals should be able to control how their personal information is used and monetized by businesses. Meanwhile, Cavoukian has developed the concept of "privacy by design," that emphasizes the need for businesses and technology developers to incorporate privacy considerations into their products and services from the outset.[1]

Despite these contributions, however, there is still much debate over how to balance cyber-security and privacy in the digital age. For instance, some scholars argue that the focus on individual privacy rights can undermine the collective good, while others contend that government surveillance and data collection can actually harm national security by eroding public trust and limiting cooperation between citizens and law enforcement agencies [O' Harrow R., 2017: 95–113].

### 1.5. Methodology

The research methodology employed in the article is a qualitative analysis of literature and legal frameworks. The purpose of the study is to pro-

[1] Cavoukian A. 2017. Privacy by design: The 7 foundational principles. Toronto, 2017.

vide an overview of the legal and ethical considerations involved in balancing cyber-security and privacy in the digital age. The study will explore the challenges of implementing cyber-security measures while respecting privacy rights and discuss the current legal framework for cyber-security and privacy in various states. In addition, the author considers the ethical implications of balancing these two important values and suggests ways in which cyber-security and privacy concerns can be reconciled in a general context. That methodology is appropriate because the topic of balancing cyber-security and privacy is complex and multi-faceted. Qualitative analysis of literature and legal frameworks is a way to examine and synthesize the current state of knowledge in this area. The methodology enables the researcher to examine multiple sources of data, identify patterns and trends, and draw conclusions based on a comprehensive analysis of the available evidence.

The approach taken in this study is based on a systematic review of the relevant literature and legal frameworks. The systematic review method involves a comprehensive and structured search of literature to identify all relevant studies. The studies are then screened and evaluated based on pre-determined inclusion and exclusion criteria. The selected studies are then analyzed and synthesized to identify key themes and patterns. The article aims to establish a methodological connection between the research objectives and the data collection and analysis methods. Methods used are designed to ensure that the research is rigorous, transparent, and replicable, and that the findings are grounded in reliable evidence. The literature review will be conducted through a systematic search of databases such as JSTOR, PubMed, and Google Scholar. The search terms used will be "cyber-security," "privacy," "legal," "ethical," and "digital age." The inclusion criteria for the literature review will be based on relevance to the research questions, quality of research, and date of publication.

### 1.6. Data Collection, Analysis, Limitations

The data collection is primarily based on a comprehensive review of literature, including books, journal articles, and other relevant publications. The literature review serves as the primary method for collecting data to support the arguments and analysis presented in the article. Author conducted a systematic search of various academic databases to identify relevant literature on the topic of balancing cyber-security and privacy in the

digital age. He used a combination of keywords and search terms related to cyber-security, privacy, digital technologies, legal and ethical considerations, and related topics to identify relevant publications. It also relied on secondary sources, including government reports, policy documents, and other relevant publications to supplement the literature review. These sources were used to provide additional insights into the current legal and regulatory frameworks for cyber-security and privacy in different countries.-

The information is reviewed and analyzed to identify the legal and ethical considerations related to cyber-security and privacy in the digital age. The analysis is conducted in a qualitative manner, where the data is grouped and categorized based on the themes and sub-themes that emerge from the literature review. The information is analyzed to identify the challenges of balancing cyber-security and privacy, the current legal framework for cyber-security and privacy in various jurisdictions, and the ethical implications of balancing these two values. The analysis is also used to identify potential ways to reconcile cyber-security and privacy concerns in a general context. The synthesis of the literature review is then presented in the article, with key findings and conclusions drawn from the analysis. The findings are presented in a logical and coherent manner with arguments and evidence to support the conclusions.

There are limitations to the study that must be acknowledged. Firstly, the study relies solely on secondary data sources, such as books, journal articles, government reports, and policy documents, and did not involve primary data collection methods, like surveys or interviews. While secondary sources provide a comprehensive overview of the topic, they may not be as nuanced as primary data sources in providing insights into specific perspectives or experiences of individuals or groups. The study focuses on legal and ethical considerations of balancing cyber-security and privacy and does not delve into technical aspects of cyber-security measures.

Future studies could explore the technical challenges of implementing strict cyber-security measures while respecting privacy rights.

Furthermore, the study focuses mainly on the Western legal framework, and more research is needed to explore the legal and ethical considerations in other parts of the world, especially in developing countries where digital technologies are rapidly growing. However, the article does not provide recommendations or solutions to the challenges identified in the study.

## 2. Cyber-security and Privacy: Definitions and Importance

### 2.1. Define Cyber-security and Privacy

Cyber-security refers to the practice of protecting computer systems, networks, and sensitive digital information from unauthorized access, theft, damage, or other malicious acts.[2] In the context of this article, cyber-security is especially important due to the proliferation of digital technologies and the increasing amount of sensitive data being collected and transmitted over the internet. The risks associated with cyber-attacks, data breaches, and other forms of digital crime are significant, and the consequences can be severe for individuals, organizations, and even entire countries. Cyber-security measures are essential for protecting privacy rights and maintaining the integrity of digital systems, but they must also be balanced against the need to respect fundamental human rights such as privacy and freedom of expression [Fisher D., 2021: 2129–2149].

The term "privacy" in the article refers to the right of individuals to control their personal information and to be free from unwanted or unwarranted surveillance or intrusion.[3] In the digital age, privacy concerns have become increasingly complex due to the vast amount of personal data that is collected, stored, and shared by individuals and bodies. This data may include sensitive information like financial records, medical histories, and personal communications, making it critical to ensure that privacy is protected. The article explores the legal and ethical considerations involved in balancing the need for privacy with the need for cyber-security measures, highlighting the importance of striking a careful balance between these two values [Stevens A., 2022: 45–77].

### 2.2. The Importance of Cyber-security and Privacy in the Digital Age

Cyber-security and privacy now are two fundamental values that are essential for individuals, businesses, and governments. Cyber-security is

[2] Rouse M. What is cyber-security? Definition, best practices & job titles. 2018. Available at: https://searchsecurity.techtarget.com/definition/cybersecurity (assessed: 18.04.2023)

[3] Universal Declaration of Human Rights, specifically Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."

important because it involves protecting sensitive information, such as personal data, financial records, and intellectual property, from unauthorized access, theft, or damage [Luiijf E., Douma A., 2019: 3–14]. Without proper cyber-security measures in place, individuals and organizations are vulnerable to cyber-attacks, which can result in financial loss, reputational damage, or legal liability. Privacy, on the other hand, is equally important because it involves protecting an individual's right to control their personal information and how it is used. In today's digital age, individuals generate and share vast amounts of personal information online, through social media, e-commerce platforms, and other digital channels. This information can be used by companies and governments for various purposes, such as targeted advertising, market research, or national security. However, it can also be misused, leading to identity theft, stalking, or other forms of harassment. [4] Balancing cyber-security and privacy is crucial because these two values often conflict with each other. For instance, implementing strong cyber-security measures may require collecting and analyzing large amounts of personal data, which could infringe on an individual's privacy rights. Conversely, protecting an individual's privacy may require limiting the collection and use of personal data, which could compromise cyber-security [Rosenzweig P., 2015: 318–329].

Therefore, finding right balance between cyber-security and privacy is essential to ensure that individuals and organizations can benefit from the opportunities offered by digital technologies, while also protecting their rights and interests. This requires a careful consideration of legal, ethical, and technical issues, as well as the development of policies and regulations to guide the use of digital technologies in a responsible and ethical manner.

### 2.3. Potential Conflicts between Cyber-security and Privacy

The challenge in balancing cyber-security and privacy is to find the right strategy between maintaining a high level of security while also respecting individuals' privacy rights. This requires a multi-faceted approach that involves implementing security measures, educating users on cyber-security risks, and developing a legal and regulatory framework that protects both cyber-security and privacy. Potential conflicts can arise between cyber-security and privacy because both concepts have distinct goals that can sometimes clash. Cyber-security focuses on protecting computer systems

[4] Singer N., Helft M. Your data is crucial to a $200 billion industry. Available at: https://www.nytimes.com/2019/03/30/opinion/sunday/data-privacy.html (assessed: 18.04.2023)

and networks from unauthorized access, theft, or damage. This involves implementing various measures such as firewalls, encryption, and access controls to prevent cyber-attacks. On the other hand, privacy is concerned with protecting personal information, such as individual identities, financial details, and online activities, from unauthorized disclosure, surveillance, or exploitation.[5]

However, cyber-security measures can potentially compromise privacy by collecting or disclosing sensitive information without the user's knowledge or consent. For example, a company might use tracking cookies to monitor a user's online behavior in order to improve their cyber-security, but this could also violate the user's privacy rights. Similarly, governments might use surveillance techniques such as wiretapping or data interception to detect potential cyber-threats, but this could also infringe on individuals' privacy rights [Villeneuve E., 2022: 495–511].

Another potential conflict is the trade-off between security and convenience. Often, cyber-security measures such as multi-factor authentication or password complexity requirements can be seen as cumbersome and time-consuming for users. This can lead to frustration and may result in users bypassing security measure altogether, which in turn compromises security. Alternatively, reducing security measures to enhance convenience can make systems vulnerable to attacks and increase the risk of data breaches.

### 2.4. Legal Framework for Cyber-security and Privacy

The legal framework varies across different jurisdictions, but there are some common principles and regulations that are widely recognized. In the United States, for example, the main legislation governing cyber-security and privacy is the Cyber-security Information Sharing Act (CISA)[6] and the Electronic Communications Privacy Act (ECPA).[7] The European Union has implemented the General Data Protection Regulation (GDPR), which provides a comprehensive framework for data protection and pri-

[5] Iqbal M. Cyber-security vs. privacy: Protecting both in the digital age. Available at: https://www.forbes.com/sites/forbestechcouncil/2019/09/24/cybersecurity-vs-privacy-protecting-both-in-the-digital-age/?sh=3d01f7af5e11 (assessed: 18.04.2023)

[6] Cyber-security Information Sharing Act of 2015. Pub. L. No. 114-113, 129 Stat. 2242. Available at: https://www.congress.gov/bill/114th-congress/senate-bill/754 (assessed: 18.04.2023)

[7] Electronic Communications Privacy Act. Pub. L. No. 99-508, 100 Stat. 1848.1986. Available at: https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf (assessed: 18.04.2023)

vacy.[8] Other countries have also enacted laws and regulations to protect personal data and secure digital infrastructure, such as the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada and the Cyber Security Law in China.[9] [10]

### 2.5. Current Legal Framework for Cyber-security and Privacy in Various Jurisdictions

In the US there are several laws and regulations that govern cyber-security and privacy. The most significant legislation is the Cyber-security Information Sharing Act (CISA) enacted in 2015 to encourage information sharing between the government and private entities regarding cyber threats. Other important laws include the Electronic Communications Privacy Act (ECPA), which regulates the interception of electronic communications, and the Health Insurance Portability and Accountability Act (HIPAA), establishing privacy standards for health information.[11] The Federal Trade Commission (FTC) has been active in enforcing privacy and data security regulations, particularly with regard to consumer protection.[12] The legal framework for cyber-security and privacy in the United States is complex and evolving, with a mix of federal and state laws, regulations, and guidelines that apply to different industries and sectors.

The current legal framework for cyber-security and privacy in Europe is primarily governed by the General Data Protection Regulation (GDPR),

[8] 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). Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (assessed: 18.04.2023)

[9] Government of Canada. 2018. Personal Information Protection and Electronic Documents Act (PIPEDA). Available at: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/ (assessed: 18.04.2023)

[10] National People's Congress. 2016. Cyber Security Law. Available at: http://www.npc.gov.cn/englishnpc/c23934/201706/a9a818170f9247d2b7294fe4cd20fadd.shtml (assessed: 18.04.2023)

[11] USA. Department of Health and Human Services (n.d.). Health Insurance Portability and Accountability Act (HIPAA). Available at: https://www.hhs.gov/hipaa/index.html (assessed: 18.04.2023)

[12] Federal Trade Commission. (n.d.). Privacy & Security. Available at: https://www.ftc.gov/tips-advice/business-center/privacy-and-security (assessed: 18.04.2023)

in effect in May 2018. The GDPR applies to all businesses operating within the European Union (EU) and regulates the processing of personal data of individuals within the EU. The regulation outlines strict requirements for obtaining consent, data breach notifications, and the right to be forgotten, among other provisions. The Network and Information Systems Directive (NIS Directive) requires EU member states to implement cyber-security measures for critical infrastructure and digital service providers, and to report major security incidents to national authorities.[13] The EU Cyber-security Act also establishes a framework for the certification of information and communication technology products and services. The legal framework in Europe prioritizes the protection of personal data and cyber-security while balancing these interests with the needs of businesses and national security concerns.[14]

In the United Kingdom main legislation governing cyber-security and privacy is the Data Protection Act of 2018[15], incorporating the General Data Protection Regulation (GDPR) into UK law. The GDPR provides a comprehensive framework for protecting individuals' personal data and sets out strict rules for the collection, storage, and processing of such data by organizations. The act also establishes the Information Commissioner's Office (ICO) as the regulator for data protection in the UK, with the power to enforce compliance and issue fines for non-compliance.[16] The UK has the Computer Misuse Act 1990 [17], that criminalizes unauthorized access to computer systems, hacking, and other cyber-related offences. The UK government has also recently introduced the National Cyber Security Strategy, which sets out a comprehensive approach to enhancing the country's

[13] European Commission. 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. Official Journal of the European Union, L 194/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (assessed: 18.04.2023)

[14] European Union. Cyber-security Act. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj (assessed: 18.04.2023)

[15] Data Protection Act 2018. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (assessed: 18.04.2023)

[16] ICO. 2018 Guide to the General Data Protection Regulation. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (assessed: 18.04.2023)

[17] UK Computer Misuse Act 1990. Available at: http://www.legislation.gov.uk/ukpga/1990/18/contents (assessed: 18.04.2023)

cyber-security capabilities and protecting against cyber-attacks.[18] The UK has a robust legal framework for cyber-security and privacy that seeks to balance the need for strong security measures with the protection of individuals' privacy rights.

In Canada the Personal Information Protection and Electronic Documents Act (PIPEDA) [19] is the primary legislation governing the collection, use, and disclosure of personal information by private sector organizations. It requires organizations to obtain an individual's consent before collecting, using, or disclosing their personal information, and to take reasonable measures to safeguard that information from unauthorized access, use, or disclosure. Canada's Anti-Spam Legislation (CASL) [20] regulates the sending commercial electronic messages, and the Digital Privacy Act [21] introduced several amendments to PIPEDA, including mandatory breach notification requirements for organizations. Office of the Privacy Commissioner is responsible for enforcing PIPEDA and promoting privacy rights. [22]

The United Arab Emirates (UAE) has implemented several legal measures to regulate cyber-security and privacy. One of the key instruments in this regard is the UAE Cybercrime Law criminalizing various cyber offenses, such as hacking, phishing, and spreading false information online.[23] The law also outlines punishments for violating the cyber-security of individuals or organizations, including fines and imprisonment. In addition, the UAE has established the National Electronic Security Authority (NESA), which is responsible for securing the country's critical information infra-

[18] HM Government. National Cyber Security Strategy 2016-2021. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (assessed: 18.04.2023)

[19] Personal Information Protection and Electronic Documents Act. 2000. Available at: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/index.html (assessed: 18.04.2023)

[20] Government of Canada. CASL of 2021. Available at: https://www.canada.ca/en/industry-canada/topics/information-communication-technology/protect-your-privacy/anti-spam-law.html (assessed: 18.04.2023)

[21] Digital Privacy Act, S.C. 2015. Available at: https://laws-lois.justice.gc.ca/eng/AnnualStatutes/2015_32/page-1.html (assessed: 18.04.2023)

[22] Canada. Office of the Privacy Commissioner. Available at: https://www.priv.gc.ca/en/about-the-opc/ (assessed: 18.04.2023)

[23] Federal Decree Law No. 5 of 2012 on Combating Cybercrimes. Available at: https://www.adjd.gov.ae/EN/MediaCenter/Publications/Pages/FederalDecreeLawNo5of2012onCombatingCyberCrimes.aspx (assessed: 18.04.2023)

structure and developing national cyber-security policies. [24] The UAE also recently enacted a data protection law, which regulates the processing of personal data and requires organizations to implement adequate measures to protect the privacy of individuals.[25] Despite these legal frameworks, concerns have been raised about the lack of transparency and due process in some cases related to cyber-security and privacy in the UAE.

In Singapore cyber-security and privacy are governed by a range of laws and regulations. The Personal Data Protection Act (PDPA)[26] is the main piece of legislation that regulates the collection, use, and disclosure of personal data in Singapore. The PDPA requires organizations to obtain individuals' consent before collecting, using, or disclosing their personal data and to take reasonable steps to protect that data.[27] The Cyber-security Act,[28] introduced in 2018, establishes a framework for the regulation of critical information infrastructure (CII) and provides for the sharing of information between CII owners and the government in the event of a cyber-attack.[29] The Computer Misuse Act[30] criminalizes various types of cyber-crime, including unauthorized access and hacking. The Monetary Authority of Singapore also issued a set of guidelines on technology risk management, that sets out best practices for financial institutions to manage cyber-risk. [31]

---

[24] National Electronic Security Authority. Available at: https://nesa.gov.ae/about-us/ (assessed: 18.04.2023)

[25] Federal Authority for Government Human Resources. 2020. UAE Federal Law No. (2) of 2019 on the Use of Information and Communications Technology in Health Fields. Available at: https://www.fahr.gov.ae/portal/en/about_fahr/news/28/3/2020/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D8%B9%D8%A7%D9%85%D8%A9-%D9%84%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-%D8%A7%D9%84%D8%B5%D8%AD%D9%8A%D8%A9.aspx (assessed: 18.04.2023)

[26] Personal Data Protection Commission. Singapore. 2021. Personal Data Protection Act. Available at: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview (assessed: 18.04.2023)

[27] Personal Data Protection Commission. Singapore. (n.d.). Personal Data Protection Act. Available at: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act (assessed: 18.04.2023)

[28] Cybersecurity Act. Singapore Statutes Online. Available at: https://sso.agc.gov.sg/Act/CSA2018 (assessed: 18.04.2023)

[29] Ministry of Communications and Information. Singapore. Cybersecurity Act. Available at: https://sso.agc.gov.sg/Act/CSA2018 (assessed: 18.04.2023)

[30] Computer Misuse Act (Chapter 50A). (n.d.). Singapore Statutes Online. Available at: https://sso.agc.gov.sg/Act/COMPA1993 (assessed: 18.04.2023)

[31] Singapore's Cybersecurity Laws and Regulations. RHT Law Asia. Available at: https://www.rhtlawasia.com/singapores-cybersecurity-laws-and-regulations/ (assessed: 18.04.2023)

China has a complex legal framework for cyber-security and privacy, which is heavily influenced by the country's political and social context. The Cyber-security Law of the People's Republic of China,[32] in force since 2016, provides a comprehensive regulatory framework for cyber-security. The law requires network operators to take measures to protect the security of personal information and to report cyber-security incidents to the authorities. It also empowers the Chinese government to conduct cyber-security inspections and investigations, and to take measures to prevent and respond to cyber-security threats [Liu X., 2017: 1– 20].

However, concerns have been raised about the potential impact of the law on privacy and free speech, as well as the lack of transparency and accountability in its implementation. Also, China has a range of other laws and regulations related to cyber-security and privacy, such as the Criminal Law[33], the State Secrets Law,[34] and the Internet Information Services Regulation.[35]

In Japan legal framework for cyber-security and privacy is primarily governed by the Act on the Protection of Personal Information (APPI)[36] revised in 2020 to strengthen privacy protections for individuals. The APPI applies to both private and public sector organizations and sets out requirements for the collection, use, and disclosure of personal information, as well as the establishment of security measures to protect against unauthorized access, loss, destruction, alteration, or disclosure of personal information. In addition to the APPI, Japan has also implemented the Cyber-security Basic Act[37]; its aims are to ensure security of information and communications

[32] National People's Congress. Cyber-security Law of the People's Republic of China. Available at: http://www.npc.gov.cn/englishnpc/Law/2017-11/07/content_2039783.htm (assessed: 18.04.2023)

[33] Criminal Law of the People's Republic of China (1997, amended 2018). Available at: http://www.npc.gov.cn/npc/c30834/201807/d53b2ae7c2474f0faa8c6a312bffb3dd.shtml (assessed: 18.04.2023)

[34] National People's Congress. Law on Guarding State Secrets. Available at: http://www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383868.htm (assessed: 18.04.2023)

[35] National People's Congress. Decision of the Standing Committee of the National People's Congress on Maintaining Internet Security. Available at: http://www.npc.gov.cn/wxzl/gongbao/2000-12/15/content_5004607.htm (assessed: 18.04.2023)

[36] Ministry of Internal Affairs and Communications of Japan. (n.d.). Act on the Protection of Personal Information. Available at: http://www.soumu.go.jp/main_content/000327861.pdf (assessed: 18.04.2023)

[37] National Diet of Japan. 2014 Act on the Establishment of the Cybersecurity Basic Act. Available at: https://www.japaneselawtranslation.go.jp/law/detail/?id=3156&vm=04&re= (assessed: 18.04.2023)

networks, and the Act on the Protection of Specially Designated Secrets[38] regulating the handling of confidential information related to national security. The Japanese government has also established the Cyber-security Strategy Headquarters to promote cyber-security measures and coordinate efforts among relevant agencies and organizations.[39]

In South Korea the Personal Information Protection Act (PIPA) serves as the primary legislation governing data privacy and cyber-security.[40] The PIPA aims to protect personal information by regulating its collection, storage, use, and provision to third parties. It also mandates the implementation of appropriate security measures to prevent data breaches and requires prompt notification of affected individuals in case of any security incidents. In addition, the Network Act requires Internet service providers to retain user data for a certain period and grants law enforcement agencies access to this data under circumstances indicated in the Act.[41] It also prohibits cyber-bullying and the spreading of false information online. The South Korean government has also established the Ministry of Science and ICT and the Korea Internet & Security Agency to oversee and regulate cyber-security measures in the country.[42] [43] Despite these regulations, there have been concerns over government surveillance and censorship in South Korea, particularly in the context of national security.

Australia has a comprehensive legal framework for cyber-security and privacy. The Privacy Act of 1988 sets out the Australian Privacy Principles (APPs), which regulate the collection, use, and disclosure of personal information by government agencies and private organizations.[44] The Privacy

[38] National Diet of Japan. 2013 Act on the Protection of Specially Designated Secrets. Available at: https://www.japaneselawtranslation.go.jp/law/detail/?id=3157&vm=04&re= (assessed: 18.04.2023)

[39] Government of Japan. Cabinet Secretariat. 2013. Cybersecurity Basic Plan. Available at: https://www.nisc.go.jp/eng/pdf/CybersecurityBasicPlan_ver2.0.pdf (assessed: 18.04.2023)

[40] National Law Information Center. 2011 Personal Information Protection Act. Available at: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=28399&lang=ENG (assessed: 18.04.2023)

[41] National Law Information Center. 2011 Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. Available at: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=29566&lang=ENG (assessed: 18.04.2023)

[42] Ministry of Science and ICT. (n.d.). About MSIT. Available at: https://english.msit.go.kr/english/main/main.do (assessed: 18.04.2023)

[43] Korea Internet & Security Agency. (n.d.). KISA Overview. Available at: https://www.kisa.or.kr/eng/main.jsp (assessed: 18.04.2023)

[44] Federal Register of Legislation. Privacy Act 1988. Available at: https://www.legislation.gov.au/Details/C2018C00243 (assessed: 18.04.2023)

Act also establishes Office of the Australian Information Commissioner responsible for enforcing the APPs and promoting privacy rights.[45] In addition, the Cyber Security Strategy 2020 outlines Australia's approach to cyber-security; it includes enhancing the resilience of critical infrastructure, promoting cyber-awareness, and strengthening law enforcement capabilities.[46] The Australian Signals Directorate (ASD) also provides guidance on cyber-security best practices for government agencies and critical infrastructure operators.[47] Australia's legal framework aims to balance the need for effective cyber-security measures with the protection of individuals' privacy rights.

The legal framework for cyber-security and privacy in South America states varies from one country to another. Brazil has implemented the General Data Protection Law to regulate the processing of personal data and protect privacy rights, which came into effect in September 2020.[48] The law applies to all businesses that process personal data, regardless of where the business is located. Mexico has the Federal Law on Protection of Personal Data Held by Private Parties, which also regulates the processing of personal data and gives individuals the right to access, correct, cancel, and object to the use of their data.[49] However, despite having legal frameworks in place, both countries still face challenges in effectively enforcing these laws and protecting the privacy of their citizens. Other South American countries such as Argentina and Chile also have legal frameworks for cyber-security and privacy, but the level of implementation and enforcement varies by country.

### 2.6. The Weaknesses of Legal Frameworks

One weakness of the legal framework for cyber-security and privacy in the USA is the lack of a comprehensive federal privacy law. While some laws and regulations (HIPAA and the Children's Online Privacy Protection

[45] Office of the Australian Information Commissioner (n.d.). Available at: https://www.oaic.gov.au/about-us/about-the-oaic/ (assessed: 18.04.2023)

[46] Department of Home Affairs. Australia's 2020 Cyber Security Strategy. Available at: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy (assessed: 18.04.2023)

[47] Australian Signals Directorate. (n.d.). Cyber security guidance. Available at: https://www.cyber.gov.au/acsc/guidance (assessed: 18.04.2023)

[48] Brazilian Presidency of the Republic. 2018 Lei Geral de Proteção de Dados Pessoais (LGPD). Available at: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm (assessed: 18.04.2023)

[49] Mexican Congress. 2010 Federal Law on Protection of Personal Data Held by Private Parties. Available at: http://www.diputados.gob.mx/LeyesBiblio/pdf/316.pdf (assessed: 18.04.2023)

Act–COPPA), address specific privacy issues, there is no overarching federal law that provides a uniform standard for data privacy and protection.[50] [51]This may lead to confusion and inconsistency for both consumers and businesses. Another weakness is the fragmentation of laws and regulations across different industries and sectors. For example, financial institutions are subject to different regulations than healthcare providers or retailers. This is able to create challenges for businesses that operate across multiple industries or sectors, as they must comply with a patchwork of laws and regulations [Brennan-Marquez K., Hoffman S., 2022: 9–55].

Additionally, the legal framework may not keep pace with technological developments and new forms of cyber threats. As technology continues to evolve at a rapid pace, it is difficult for lawmakers and regulators to keep up with the latest trends and issues. It leads to gaps in the legal framework and potentially leave individuals and businesses vulnerable to cyber-attacks and privacy violations. There may be a lack of enforcement and penalties for non-compliance with cyber-security and privacy regulations. While the FTC has been active in enforcing privacy and data security regulations, there have been instances where companies have suffered data breaches or other privacy violations without facing significant consequences. It may create a perception that there is a low risk of punishment for non-compliance, which may not incentivize companies to prioritize cyber-security and privacy [Hickman L., Martin C., 2022: 73–132].

One potential weakness of the European legal framework in the field is that it may not be able to keep pace with rapidly evolving technologies and cyber threats. The GDPR, for example, was drafted prior to the widespread adoption of emerging technologies such as artificial intelligence and the Internet of Things, which present new challenges for data protection and cyber-security. The regulation has been criticized for being overly prescriptive and burdensome for businesses, particularly small and medium-sized enterprises. There is also concern that the GDPR may be difficult to enforce consistently across EU states; it could result in varying levels of protection for personal data and cyber-security in different countries. The legal framework may not be sufficient to address the challenges posed by cyber threats

[50] US Congress. Health Insurance Portability and Accountability Act of 1996. Available at: https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm (assessed: 18.04.2023)

[51] US Congress. 1998 Children's Online Privacy Protection Act. Available at: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (assessed: 18.04.2023)

that originate from outside of the EU, highlighting the need for international cooperation and coordination on cyber-security and privacy issues [Purcell R., 2021: 135–148].

One weakness of the legal framework for cyber-security and privacy in the UK is the impact of Brexit on the applicability of the GDPR. While the Data Protection Act 2018 incorporates the GDPR into UK law, there is still uncertainty around how the UK's departure from the EU will affect the regulation's enforcement and application [White L., 2021: 8–10]. Additionally, the Computer Misuse Act 1990 has been criticized for being outdated and not providing sufficient protections against emerging cyber threats, such as those posed by nation-states or sophisticated criminal organizations. There is also the potential for conflicts between the UK's national security interests and individuals' privacy rights, which may lead to challenges in balancing the two priorities.[52] While the UK has a relatively robust legal framework for cyber-security and privacy, there is room for improvement and adaptation to meet the evolving challenges of the digital age.

One weakness of Canada's legal framework in the area is that PIPEDA only applies to private sector bodies, leaving government entities largely outside its scope. This means that government agencies may not be subject to the same strict requirements for data protection and privacy as private businesses.[53] While PIPEDA requires organizations to take reasonable measures to safeguard personal information, it does not provide specific guidance on what constitutes "reasonable measures," leaving room for interpretation and potential inconsistencies in compliance. Some critics have argued that Canada's privacy laws do not go far enough in protecting individuals' privacy rights, particularly in the face of evolving technologies and new threats to digital privacy [Rideout V., 2022: 83–85].

One weakness of the legal framework for cyber-security and privacy in the UAE is the lack of clarity and consistency in several laws and regulations. For example, the UAE Cybercrime Law has been criticized for its vague and broad language, which could lead to overreach and abuse of

[52] Henderson E. The UK's approach to cyber-security is weak — and now it's an international problem. The Guardian. Available at: https://www.theguardian.com/commentisfree/2022/jan/31/uk-cybersecurity-international-problem-britain-cyber-attacks. (assessed: 18.04.2023)

[53] Furuta K. Canadian privacy overhaul: what you need to know about Bill C-11. Harvard Business Review. 2021. Available at: https://hbr. org. 2021/02/canadas –privacy-overhaul-what-you-need-to-know-about-bill-c-11 (assessed: 18.04.2023)

power [Al-Fadhli N., 2021: 18–25]. In addition, while the data protection law is a positive step towards protecting individuals' privacy, some have raised concerns about the lack of a comprehensive regulatory framework and the potential for arbitrary enforcement. Another weakness is the limited transparency and due process in some cases related to cyber-security and privacy, which could undermine trust in the legal system and discourage individuals and bodies from reporting incidents or seeking justice [Abdul-Kareem A., 2021: 105488]. These shortcomings highlight the need for continued strengthening and refining legal frameworks in the UAE, with a focus on clarity, consistency, transparency, and due process.

While Singapore has implemented a comprehensive legal framework in the field, there are still some weaknesses to be addressed. One criticism of the PDPA is that it does not provide for a private right of action, which means that individuals cannot sue bodies for damages resulting from violations of the act [Dhamija R., 2022: 107937]. Another issue is that the government's powers under the Cyber-security Act have been criticized for being too broad and potentially infringing on individuals' privacy rights. Additionally, there have been concerns raised about the lack of transparency and accountability in the government's use of surveillance technologies.

These issues highlight the need for ongoing review and reform of Singapore's legal frameworks to ensure they strike an appropriate balance between protecting individuals' rights and promoting national security and economic interests.

Weakness of China's legal frameworks is the lack of transparency and accountability in their implementation. The Chinese government has broad powers to regulate and monitor online activity, and there have been concerns about the potential for these powers to be abused for political purposes [Zhang Y., 2021: 519–540]. The lack of clear and consistent enforcement mechanisms for cyber-security and privacy laws also raises questions about their effectiveness in practice. The strict regulatory environment in China can create barriers to innovation and entrepreneurship, as well as limit free expression and access to information online. The complex and often overlapping nature of China's legal frameworks for cyber-security and privacy can create confusion and uncertainty for both individuals and organizations operating in the country [Sun R., Xu Q., 2021: 103341].

One of the weaknesses of Japan's legal framework in the field is that the APPI's enforcement mechanisms may be insufficient to deter non-compliance. The APPI relies heavily on self-regulation and voluntary compliance

by organizations, with the Personal Information Protection Commission (PPC) responsible for enforcement. However, the PPC has limited powers to impose penalties on non-compliant organizations, and its authority to investigate violations is also restricted. In addition, the Cyber-security Basic Act and the Act on the Protection of Specially Designated Secrets primarily focus on protecting national security and critical infrastructure, which may limit their effectiveness in addressing broader cyber-security and privacy concerns. While Japan has made efforts to strengthen its legal framework for cyber-security and privacy, there may be room for further improvement in terms of enforcement and scope [Izumi K., 2021: 1–23].

South Korea has implemented various laws and regulations to regulate data privacy and cyber-security, nonetheless there are some weaknesses in the legal framework. One concern is the too broad surveillance powers granted to law enforcement agencies under the Network Act, which could potentially violate individuals' privacy rights. Another issue is the potential for government censorship, particularly in the context of national security, which could limit individuals' freedom of expression. There have been criticisms that the penalties for violating data privacy regulations under the PIPA are not severe enough to act as a sufficient deterrent. There have been concerns about the effectiveness of the regulatory bodies established to oversee cyber-security measures, particularly in the face of increasingly sophisticated cyber-threats [Kim M., Kim Y., 2021: 2675–2692].

Australia's legal framework is comprehensive; there have been concerns about its purpose in practice. One weakness is that the Privacy Act and APPs only apply to government agencies and private organizations with an annual turnover of more than AUD 3 million, meaning that smaller organizations may not be subject to the same level of regulation [Patterson M., 2021: 825–857]. In addition, there have been criticisms of the OAIC's enforcement powers and the adequacy of its resources to effectively regulate and enforce privacy protections. The Cyber Security Strategy 2020 has also faced criticism for being too focused on national security and not sufficiently addressing the broader cyber-security concerns of individuals and businesses. The effectiveness of the ASD's guidance on cyber-security best practices has been questioned, with some experts arguing that it may not be sufficient to address the evolving and sophisticated cyber threats facing Australia [Chia P., Teo T., 2021: 102307].

The weakness of the legal frameworks in the field in South America is the lack of strong enforcement mechanisms. While jurisdictions like Brazil

and Mexico have laws to protect personal data and privacy, there are challenges in enforcing these laws. This can be due to a variety of factors: limited resources for regulatory bodies, weak penalties for non-compliance, and lack of awareness and understanding of the laws by both individuals and businesses. The level of implementation and enforcement vary between different regions and sectors within a country. As a result, individuals and businesses may not feel compelled to comply with the regulations, leading to potential breaches of privacy and cyber-security threats. To address these weaknesses, there is a need for stronger enforcement mechanisms, as well as increased awareness and education about the importance of protecting personal data and privacy [Schaerer E., 2022: 111-125].

### 2.7. Gaps or Inconsistencies in the Legal Frameworks

One significant gap in the legal framework in the United States is the lack of comprehensive federal privacy legislation. While there are several laws that regulate privacy in specific sectors, such as HIPAA for healthcare and the Children's Online Privacy Protection Act (COPPA) for children's data, there is no overarching federal law that provides a comprehensive framework for privacy protection. This has led to a patchwork of state laws, such as the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (CDPA), that have been enacted to fill the gap [Hu M., 2021: 501–534]. Another inconsistency is the tension between national security interests and privacy rights, particularly in the context of government surveillance programs. While CISA encourages information sharing to protect against cyber threats, it has also been criticized for potentially infringing on privacy rights. The legal framework for cyber-security and privacy in the US is fragmented and lacks a cohesive approach to privacy protection [Wessel M., van der Sloot B., 2021: 167–183].

In the legal framework for cyber-security and privacy in Europe is the lack of a unified approach to cyber-security and data protection across all member states. While the GDPR provides a comprehensive framework for data protection, the implementation and enforcement of the regulation can vary widely between member states. There is a lack of harmonization between the GDPR and other regulations, such as the NIS Directive that is able to lead to confusion and inconsistencies in compliance requirements [Van Eecke P., Oberschelp de Meneses A., 2021: 293–307].

Another potential gap is the lack of clear guidance on cross-border data transfers, particularly in light of the Schrems II decision by the European

Court of Justice invalidating the EU-US Privacy Shield Framework. These gaps can create challenges for businesses operating across borders and can lead to regulatory uncertainty and legal disputes [Hirila-Rus A., Borza A., 2022: 1–6].

One potential gap in the United Kingdom legal framework is the lack of specific regulations for the Internet of Things devices. As these devices become more prevalent, they may pose significant cyber-security risks and privacy concerns. Another potential gap is the limited scope of the Data Protection Act 2018, which applies only to data processing activities that are conducted within the UK. This may leave gaps in protection for individuals' personal data that is processed by organizations based outside of the UK. There have been concerns raised about the adequacy of fines imposed by the ICO for data breaches, which some argue may not be sufficient to deter non-compliance with data protection regulations [Thomas M., 2021: 6–9].

As for Canada, here PIPEDA applies to the private sector only, leaving government agencies and departments without a consistent privacy protection framework. There are concerns that PIPEDA may not provide sufficient protection for individuals' privacy rights in the face of swiftly progressing technology and cyber threats. Some critics have called for stronger enforcement powers for the Privacy Commissioner of Canada, as well as amendments to PIPEDA to ensure that it remains relevant and in protecting Canadians' privacy in the digital age.[54]

Gap in the field in the UAE is the possible conflict between the UAE Cybercrime Law and laws related to freedom of expression and human rights. Critics have raised concerns that the broad language of the law could be used to target individuals who express dissenting opinions or criticize the government. Additionally, there have been reports of individuals being detained or prosecuted for online activity that would be considered protected speech in other countries. Furthermore, the lack of transparency and due process in some cases raises concerns about the potential for abuse of power and infringement on individuals' rights to privacy and fair trial [Shafiq M., 2022: 14].

While Singapore has comprehensive legal frameworks in the field, some gaps and inconsistencies remain. For instance, the Cyber-security Act only

[54] Layton J. Privacy commissioner flags potential privacy gaps in the government use of AI. 2021. Available at: https://www. itworldcanada.com/article /privacy-commissioner-flags-potential-privacy- gaps-in government-use-of-ai (assessed: 18.04.2023)

applies to designated CII sectors, which excludes many bodies that could be vulnerable to cyber-attacks. This leaves gaps in the regulation of cyber-security measures for non-CII organizations. The PDPA has been criticized for being too lenient towards organizations that violate privacy laws, as fines for non-compliance are relatively low. Another potential inconsistency is the lack of clarity regarding the extent to which government agencies may access personal data for national security purposes. This could potentially lead to privacy violations if personal data is accessed without due process [Leong K., 2021: 105484].

In China one of the main gaps and inconsistencies in the legislation is the lack of transparency and accountability in its implementation. This has raised concerns about abuse of power by government authorities and the potential for violations of individuals' privacy and free speech rights. The Cyber-security Law grants broad powers to the government to regulate and control information flow online, which has led to criticism from human rights groups and tech companies alike. Some of the other laws and regulations related to cyber-security and privacy like the State Secrets Law, also have been criticized for their vague and broad definitions, which could be used to justify the persecution of individuals and groups for political or ideological reasons [Zheng Y., 2021: 102156].

While South Korea has made efforts to strengthen its legal frameworks, there are still gaps and inconsistencies that need to be addressed. One major concern is the potential for government surveillance and censorship, particularly in the context of national security. The Network Act grants law enforcement agencies access to user data under certain circumstances, which has raised questions about the extent of government surveillance in South Korea. Similarly, there have been cases where South Korean authorities have been accused of censoring online content, which raises concerns about the potential impact on freedom of expression. Furthermore, the efficiency of the PIPA in protecting personal data has been called into question, as data breaches continue to occur in the country. Therefore, there is a need for further reforms and improvements in South Korea's legal frameworks [Joo S., 2022: 23–27].

### 2.8. Challenges of Implementing Effective Cyber-security Measures While Respecting Privacy Rights

The increasing reliance on digital technologies and the internet has made cyber-security a critical concern for individuals, businesses, and gov-

ernments worldwide. However, it is equally essential to protect individuals' privacy rights while implementing strict cyber-security measures. This requires finding a balance between collecting the necessary data for cyber-security purposes and avoiding excessive data collection or misuse of personal information. It is crucial to determine which types of data are relevant and necessary for cyber-security purposes and ensure that sensitive data is protected adequately. Finding this balance is a complex task that requires collaboration of businesses, governments, and individuals to ensure that cyber-security and privacy are protected simultaneously [Xu H., Zhang R., 2021: 9–12].

In implementing cyber-security measures it is crucial to ensure that the collection and use of personal data are limited to what is necessary for cyber-security purposes. Excessive data collection or misuse of personal information could violate privacy rights, and it is essential to strike a balance between collecting enough information to protect against cyber threats while not infringing on privacy. Organizations should limit their data collection practices to the minimum necessary for cyber-security and implement appropriate safeguards to prevent misuse or unauthorized access to personal information. By doing so, they are able to protect both cyber-security and privacy rights and maintains trust with their customers or users.

Determining types of data necessary for cyber-security purposes is another challenge in implementing reasonable cyber-security measures while respecting privacy rights. While some information such as login credentials and IP addresses are essential for detecting and preventing cyber-attacks, other types of personal data such as browsing history or location data may not be necessary for cyber-security purposes and could be considered a violation of privacy rights. Bodies need to have a clear understanding of the data that they collect, the reasons for its collection, and how it will be used and stored. They should only collect data that is necessary for cyber-security purposes, and any personal data that is collected should be anonymized or encrypted to protect privacy.

Another challenge in implementing cyber-security measures while respecting privacy rights is finding a balance between the two, as privacy regulations and cyber-security needs often conflict with each other. For example, regulations such as GDPR and CCPA require companies to obtain user consent before collecting and processing personal data, while cyber-security measures may require continuous monitoring and analysis of user data to detect and prevent cyber-attacks. Companies must comply with these

regulations while still ensuring the protection of their cyber-security. This can be achieved by implementing privacy policies that outline data collection, use, and storage practices, obtaining user consent for data collection, and using technologies such as encryption and anonymization to protect personal data [Ghosh D., Scott M., 2022: 105666].

Implementing strict cyber-security measures while protecting sensitive data like medical records or financial information, is a significant challenge. These types of data require a higher level of protection due to the severe consequences that could result from a breach. However, ensuring the security of sensitive data must also be balanced with the need to respect privacy rights. Organizations must ensure that they are collecting only the necessary data for cyber-security purposes, using appropriate encryption and access controls to protect the data, and complying with relevant regulations such as HIPAA or PCI DSS. They must also provide transparency to users about how their data is being collected, stored, and used. By balancing these needs, organizations can ensure that sensitive data is protected while still respecting privacy rights.[55]

Implementing cyber-security measures while respecting privacy rights is a challenging task. It requires a thorough understanding of both cyber-security and privacy regulations and a collaborative effort of business, powers, and individuals. Organizations must collect only the necessary data for cyber-security purposes, protect sensitive data, and comply with relevant privacy regulations while still ensuring the protection of their cyber-security. Users must also be educated on the importance of cyber-security and privacy and provided with transparency about data collection and use practices. By working together and finding the right balance between cyber-security and privacy, organizations can protect against cyber threats while respecting individuals' privacy rights [Mangla S., 2021: 49–62].

### 2.9. Challenges Involved in Balancing Cyber-security and Privacy in Practice

One of the main challenges is limited resource. Many bodies, particularly small businesses, have a limited budget or staff to allocate to cyber-security and privacy measures. This can make it challenging to implement robust

[55] Fowler K. Balancing privacy and cyber-security when securing sensitive data. 2021. Available at: https://securityintelligence.com/articles/balancing-privacy-and-cybersecurity-when-securing-sensitive-data/ (assessed: 18.04.2023)

security measures that protect against cyber threats while also respecting privacy rights. Organizations may need to prioritize their resources based on their most significant security risks and compliance requirements. For example, they may choose to implement basic security measures such as strong passwords and regular software updates and focus on complying with relevant privacy regulations. It is crucial to allocate sufficient resources to cyber-security and privacy to ensure that both areas are adequately protected. [Kharraz A., Robertson W. et al. 2021: 13–23].

Another significant challenge in balancing cyber-security and privacy is navigating complex privacy regulations, such as GDPR or CCPA. These regulations can be challenging to understand and comply with, particularly for organizations with limited legal expertise. Compliance with privacy regulations is critical to protect individuals' privacy rights, but it can be challenging to implement effective cyber-security measures while complying with these regulations. Organizations may need to seek legal advice to ensure they are compliant while also implementing robust cyber-security measures that protect against cyber threats. It is crucial to have a clear understanding of privacy regulations to ensure that both privacy and cyber-security are adequately protected.[56]

Lack of awareness and education is another significant challenge in balancing cyber-security and privacy. Many individuals and businesses do not fully understand the importance of cyber-security or privacy, which can make it challenging to implement effective measures. Users may not be aware of the risks of cyber threats or the importance of protecting their personal data. This can result in poor security practices, such as weak passwords or sharing sensitive information with untrusted parties. Bodies may need to provide training and education to their employees to ensure they understand the importance of cyber-security and privacy and how to implement effective measures. Users may also need to be educated on best practices for protecting their personal data and privacy online, such as avoiding phishing scams and using strong passwords. Increasing awareness and education on these issues is critical to balancing cyber-security and privacy effectively.[57]

[56] Lee Y. et al. Can Privacy Regulations Improve Cyber-security? A Preliminary Empirical Study. 2021. Proceedings of the 54th Hawaii International Conference on System Sciences, pp. 3552–3561. Available at: https://doi.org/10.24251/HICSS.2021.440. (assessed: 18.04.2023)

[57] Madden M. et al. Parents, teens, and online privacy. Available at: https://www.pewresearch.org/internet/2013/05/21/parents-teens-and-online-privacy/ (assessed: 18.04.2023)

Technical complexity is another challenge in balancing. Implementing cyber-security measures may be technically complex and require specialized knowledge and expertise. It may be challenging for organizations to find the necessary expertise to implement robust cyber-security measures while also protecting privacy. Cyber-security measures may involve implementing complex technical solutions, such as firewalls, intrusion detection systems, and encryption, which require specialized knowledge and expertise to set up and manage adequately. Bodies may need to hire cyber-security professionals or outsource their cyber-security needs to third-party providers to ensure they have the necessary expertise to implement effective measures while also protecting privacy. It is crucial to have the technical knowledge and expertise necessary to implement robust cyber-security measures that protect against cyber threats while also respecting privacy rights [Rass S., Chiumento A., Engel T., 2021: 17].

Balancing privacy and security needs is one more challenge. There can be a tension between privacy and security needs, as the measures needed to protect against cyber threats may conflict with privacy requirements. For example, collecting and analyzing user data may be necessary for detecting and preventing cyber-attacks, but it may also raise privacy concerns. Similarly, encryption and other security measures may be necessary to protect sensitive data, but they may also make it challenging to access data for legitimate purposes [Gürses S., Troncoso C., 2022: 78–84]. Organizations need to find the right balance between privacy and security needs, ensuring that cyber-security measures work also respecting privacy rights. This may involve implementing technical and organizational measures that minimize the collection and use of personal data and ensuring that any data collected is used only for legitimate cyber-security purposes. It is crucial to find the right balance between privacy and security to ensure that bodies can effectively protect against cyber threats while also respecting privacy rights [Mendes R., Bonneau J., 2022: 78–89].

### 2.10. Potential Impact of Cyber-security Measures on Privacy Rights

That impact is a significant concern, as cyber-security measures often involve collecting and analyzing personal data that could be considered a violation of privacy rights. It can lead to concerns over the potential misuse of personal information or the creation of a surveillance state. For instance, the collection of internet activity data could reveal sensitive information

about an individual's political views, health conditions, or personal relationships, which could be exploited for nefarious purposes. Additionally, the use of facial recognition technology or other biometric data for authentication or security purposes could raise privacy concerns regarding potential misuse of sensitive information.[58]

The collection and processing of personal data for cyber-security purposes can have an enormous impact on privacy rights, as individuals may not be aware that their personal data is being collected, processed, and analyzed. This lack of transparency and consent can lead to concerns over the potential misuse of personal information. Furthermore, the storage and processing of personal data for cyber-security purposes may also raise concerns about data security. Cyber-security systems are not invulnerable to cyber-attacks, and if such systems are breached, personal data may be exposed, leading to significant harm and privacy violations. Therefore, it is essential to implement strong data security measures to protect personal data and ensure that privacy rights are respected [Choo K.-K., Tan H., 2021: 3–17].

While cyber-security measures may impact privacy rights, they can also help protect personal data from cyber threats and breaches. Cyber-attacks and data breaches can result in the exposure of personal data, leading to significant harm for individuals, such as identity theft or financial loss. Relevant cyber-security measures can prevent such attacks and breaches, ensuring that personal data is protected. The implementing strong cyber-security measures can increase user confidence in organizations' ability to protect their data, promoting privacy rights and enhancing trust in digital systems. Therefore, it is important to find a balance between cyber-security measures and privacy rights to ensure that both are adequately protected [Chakraborty R., 2021: 2727].

Balancing cyber-security and privacy is a hard task for organizations, and it requires a comprehensive approach that involves addressing the potential impact of cyber-security measures on privacy rights. By adopting a privacy-by-design approach, organizations can ensure that privacy is considered at every stage of the cyber-security process, from the design of security measures to the implementation and monitoring of security systems. That approach can help bodies to minimize the impact of cyber-security

[58] Chen B. Biometric data collection sparks privacy concerns. Wall Street Journal. 2022. Available at: https: //www.wsj.com/articles/biometric-data-cfollection-sparks-privascy-concerns-11647691800 (assessed: 18.04.2023)

measures on privacy rights, while still ensuring that personal data is adequately protected from cyber threats. Ultimately, balancing cyber-security and privacy requires a collaborative effort between organizations, individuals, and governments, and it is essential to find the right balance between these two critical areas [Koops B., Newell B. et al., 2021: 1–19].

## 3. Ethical Concerns Related to Cyber-security and Privacy

There are several ethical concerns related to the theme of the study. The use of surveillance technologies for cyber-security purposes creates ethical concerns as it raises questions about the appropriate level of monitoring that is necessary to ensure security. While surveillance technologies can help prevent cyber threats and ensure safety, the use of these technologies can also raise concerns about civil liberties and individual privacy. Organizations need to carefully consider the ethical implications of using surveillance technologies, ensuring that any monitoring is proportionate and limited to what is necessary for cyber-security purposes. The transparency and accountability measures should be in place to ensure that individuals' privacy rights are respected [Koops B. et al., 2021: 93–109].

One more ethical concern related to cyber-security and privacy is the potential misuse of personal data by organizations or individuals. Personal data collected for legitimate cyber-security purposes may be misused for other purposes, such as marketing or profiling. It raises concerns about the unauthorized use of personal data and the potential for individuals to be harmed or exploited as a result. The use of personal data in cyber-security measures could lead to a lack of transparency and accountability in how organizations handle and protect personal data, raising ethical concerns about the responsibility of organizations to protect individuals' privacy rights [Taddeo M., Floridi L., 2021: 53–54].

Data breaches and cyber-attacks are ethical concerns in cyber-security and privacy as they may result in the loss, theft, or misuse of personal data. This could lead to identity theft, financial fraud, reputational damage, and other harmful consequences for individuals. In addition, bodies that fail to adequately protect personal data may be seen as negligent and unethical, as they have a responsibility to safeguard the personal information of their customers and users. The potential harm caused by data breaches and cyber-attacks highlights the importance of ethical cyber-security practices

and the need for organizations to prioritize the protection of personal data [Kshetri N., 2021: 326–334].

Accountability and responsibility are critical ethical concerns. Organizations that collect and store personal data must be accountable for protecting that data from cyber threats and breaches. If a breach occurs, organizations must take responsibility for it, and individuals affected by the breach must be notified promptly. Failure to do so can lead to a loss of trust between the organization and its customers, and may raise ethical concerns about the body's commitment to protecting personal data. The organizations should be transparent about their cyber-security and privacy practices to maintain the trust of their customers and other stakeholders [Gross A., Acquisti A., 2021: 102260].

### 3.1. Ethical Implications of Balancing Cyber-security and Privacy

That issue highlights the need for organizations to find a balance between protecting personal data and respecting privacy rights. This involves implementing cyber-security measures that minimize the collection and use of personal data while ensuring that any data collected is used only for legitimate cyber-security purposes. Organizations must also be transparent about their cyber-security practices and take responsibility for any breaches that occur, promoting trust and accountability. It is essential to strike a balance between cyber-security and privacy to ensure that individuals' rights are respected while protecting against cyber threats [Vadlamudi P., 2022: 1–18].

Furthermore, organizations must also ensure that their cyber-security measures are not discriminatory and do not unfairly target or discriminate against certain individuals or groups. They must take steps to prevent data breaches and protect personal data from unauthorized access, use, or disclosure. At the same time, they must balance these considerations with the need for cyber-security measures to protect against cyber threats. This involves finding a balance between security and privacy that is ethical and respects the rights and interests of all bodies and human persons involved. The ethical implications of balancing cyber-security and privacy require organizations to take a comprehensive and nuanced approach to cyber-security that accounts for the diverse needs and concerns of all stakeholders involved [Bergmann M., Grohmann B., 2022: 197–207].

Addressing potential biases in cyber-security measures is necessary to ensure fairness and avoid discrimination. Bodies must implement mea-

sures to identify and mitigate any biases in algorithms and other tools used for cyber-security purposes. This may involve regular monitoring and testing to identify any patterns of bias and taking steps to correct them. Additionally, involving diverse perspectives and input in the development and implementation of cyber-security measures can help ensure that biases are identified and addressed. By doing so, organizations can ensure that their cyber-security practices are fair and just for all individuals, regardless of their demographic characteristics [López-Pozuelo J. et al., 2022: 1146–1162].

The increasing use of digital technologies and collection of personal data has significant ethical implications for society as a whole, as it affects individual rights and freedoms, as well as broader issues such as social justice and equity. There is a need to balance the benefits of technological innovation and cyber-security measures with potential risks and adverse impacts on privacy rights and other ethical considerations. It is crucial to engage in open and transparent discussions and policymaking processes that address these issues and ensure that cyber-security and privacy measures are fair, just, and equitable for all members of society [Floridi L., 2021: 20200242].

Balancing cyber-security and privacy is a complex task that requires organizations to weigh the benefits of cyber-security measures against their potential impact on privacy rights. To do so, organizations must take into account a range of ethical principles and values, including fairness, transparency, accountability, and respect for individual rights. By adopting ethical frameworks that prioritize these principles, bodies can ensure that their cyber-security measures are both strong and respectful of privacy rights. Ultimately, the ethical implications of balancing cyber-security and privacy extend beyond individual organizations to society as a whole, and it is important to consider these implications as we continue to rely on digital technologies to protect our data and infrastructure.

### 3.2. The Ethical Implications of Balancing Cyber-security and Privacy

The balancing raises several ethical considerations that organizations must address to ensure that they protect personal data while respecting individuals' privacy rights. One of the most significant ethical implications is the need to combine security and privacy in a fair and just manner. Organizations must consider the potential impact of their cyber-security measures on individuals' privacy rights and take steps to minimize any adverse

effects. They must also be transparent about their cyber-security practices and take responsibility for any breaches that occur [Barnes D., Liang X., 2022: 103598].

The potential for bias in cyber-security measures raises important ethical concerns, as it can result in unfair treatment and discrimination against individuals or groups. Algorithms and other tools used to identify potential cyber threats may use biased data or rely on assumptions that reflect societal biases, leading to incorrect assessments and unequal treatment. This can have serious consequences for individuals' rights and opportunities, and undermine the principles of fairness and justice. Therefore, organizations must ensure that their cyber-security measures are designed and implemented in a way that minimizes bias and discrimination and promotes equity and inclusivity. They must also be transparent and accountable for any biases that arise and take steps to address them. [59]

The increasing reliance on digital technologies and the collection of personal data in today's society have profound ethical implications for cyber-security and privacy. The widespread use of technology means that individuals' personal data is increasingly vulnerable to cyber threats, including data breaches and cyber-attacks. This creates a growing need for organizations to prioritize cyber-security measures to protect personal data. However, as these technologies become more prevalent, it is essential to consider their broader ethical implications for society as a whole. For instance, the collection and use of personal data by tech companies raise concerns about surveillance, privacy, and control over individuals' data. Thus, organizations must balance their cyber-security measures with ethical principles and values that uphold the privacy rights of individuals while ensuring security of personal data [Warren M., Brandeis L., 1890: 193–220].

Balancing cyber-security and privacy is a complex task that involves a range of ethical considerations. On the one hand, bodies have a responsibility to protect personal data from cyber threats that requires strict cyber-security measures. On the other hand, individuals have a right to privacy must be respected even in the context of cyber-security. They must carefully consider potential ethical implications of their cyber-security measures, such as privacy invasion and discrimination, and take steps to minimize any adverse effects [Axelsson A.-S., Söderberg J., 2022: 105639].

[59] Buolamwini J., Gebru T. Gender shades: Intersectional accuracy disparities in commercial gender classification. 2018. Conference on Fairness, Accountability and Transparency, pp. 77-91. Available at: https://doi.org/10.1145/3178876.3186151 (assessed: 18.04.2023)

They must be transparent about their cyber-security practices and take responsibility for any breaches that occur. The broader ethical implications of digital technologies and personal data collection for cyber-security and privacy must also be considered, and steps taken to address these risks and challenges. Ultimately, balancing cyber-security and privacy requires a careful consideration of ethical principles and values, including fairness, transparency, accountability, and respect for individual rights, to ensure that personal data is protected while individuals' privacy rights are respected [Floridi L., Taddeo M., 2016: 19].

### 3.3. The Potential Trade-Offs between Cyber-security and Privacy

Some cyber-security measures: two-factor authentication, password managers, and encryption, require the collection and storage of personal data to be effective. This can include sensitive information like passwords, biometric data, and location data. The collection and analysis of this data can potentially violate individual privacy rights and raise concerns about surveillance.[60] Cyber-security measures, such as firewalls and intrusion detection systems, may monitor network traffic and user activity, raising concerns about the extent to which individuals' online activities are being monitored and tracked. Balancing the need for cyber-security with respect for privacy rights requires careful consideration of the potential trade-offs involved in implementing security measures [Lips M., Stupar A., 2021: 60–75].

Strict access controls and authentication protocols can enhance cyber-security by preventing unauthorized access to sensitive data. However, these measures may also require collecting and analyzing personal information like biometric data or device identifiers; it can be seen as an invasion of privacy. A monitoring network activity to detect potential cyber threats can be useful for identifying and mitigating security risks. Still, it may also involve collecting and analyzing data on individual users' online behavior, raising concerns about surveillance and infringement of privacy. Organizations must consider the potential trade-offs between cyber-security and privacy and strive to strike a balance that protects both individual privacy rights and organizational security needs [Latham J., Sassenberg U., 2021: 1–6].

[60] Giovanella F., Perri P. Privacy Risks of Cybersecurity Measures: An Overview. IEEE Access, no. 9, pp. 93098-93115. Available at: https://doi.org/10.1109/ACCESS.2021.3096631 (assessed: 18.04.2023)

Machine learning and artificial intelligence (AI) can be powerful tools for identifying potential cyber threats and strengthening cyber-security measures. However, these technologies may also involve analyzing large amounts of personal data, which can raise ethical concerns about privacy and discrimination. For example, if algorithms are trained on biased datasets or if certain groups are underrepresented in the data, the resulting cyber-security measures may discriminate against those groups. The use of machine learning and AI may result in the creation of new types of personal data, such as behavioral biometrics, that individuals may not even be aware are being collected and analyzed. This highlights the need for transparency and accountability in cyber-security practices to ensure that individuals' privacy rights are respected [Eubanks V., 2021: 22–25]. When organizations prioritize security over convenience, they may require users to follow strict protocols to access their data, such as entering long and complex passwords or using multi-factor authentication. While these measures can enhance security, they can also be time-consuming and frustrating for users, which may affect their productivity and overall experience. Balancing security and convenience requires finding a middle ground that minimizes the impact on user experience while still ensuring adequate security measures are in place. This can involve implementing technologies such as biometric authentication or single sign-on to streamline access to data while still ensuring its security [Rizvi S., Alhadreti O., 2021: 36 -39].

Balancing cyber-security and privacy involves a trade-off between protecting sensitive data from cyber threats and respecting individuals' privacy rights. Strict security measures may require collecting and analyzing personal data; it can raise ethical concerns about surveillance and discrimination. A stringent security measures can make it difficult for individuals to access their data easily and quickly, impacting user experience and productivity. The right balance is necessary to ensure that individuals' privacy rights are respected while sensitive data is protected from cyber threats. It requires careful consideration of ethical principles and values like fairness, transparency, and accountability, and ongoing monitoring and evaluation of security measures to minimize potential trade-offs [Sharma R., Jindal A., 2022: 1–22].

### 3.4. Suggest Ways in Cyber-security and Privacy Concerns can be Reconciled

Reconciling cyber-security and privacy concerns requires a balanced approach that respects both individual privacy rights and the need for ro-

bust cyber-security. Implementing data minimization is a strategy for reconciling cyber-security and privacy concerns by limiting the amount of personal data an organization collects, processes, and stores. By collecting only the minimum amount of personal data necessary for a specific purpose, organizations can reduce the risk of data breaches and cyber threats while respecting individuals' privacy rights [Ikram N., Burnett E., 2022: 97–108]. For example, an organization can limit the collection of biometric data to only those employees who require access to secure areas, rather than collecting it from all employees. Implementing data minimization can also help organizations comply with data protection regulations like the General Data Protection Regulation and the California Consumer Privacy Act requiring organizations to collect and process personal data only for specific purposes and with individuals' consent.

Encryption is a security measure that involves transforming plaintext data into cipher text to prevent unauthorized access. By using encryption, organizations can protect sensitive data both in transit and at rest. Encryption can be used to protect data stored on servers, as well as data transmitted over networks. In this way, encryption can help reconcile cyber-security and privacy concerns by providing a high level of security while also respecting individuals' privacy rights. However, encryption is not a panacea and can be circumvented by determined attackers. Therefore, it should be used in conjunction with other security measures to provide a layered defense [Sundararajan M., 2022: 002].

Fostering a culture of privacy is an essential way to reconcile cyber-security and privacy concerns. By promoting privacy as a core value and training employees on privacy best practices, organizations can create a culture that values privacy and respects individuals' rights. Policies such as privacy impact assessments, privacy notices, and data protection policies can also help demonstrate a commitment to privacy. The organizations can appoint a data protection officer to oversee privacy compliance and facilitate communication between employees, customers, and other stakeholders. By prioritizing privacy in their operations, organizations can build trust with customers and stakeholders and demonstrate a commitment to protecting personal data [Rosenberg Y., 2021: 36–42].

A privacy impact assessment (PIA) is a tool that organizations can use to assess the potential impact of new cyber-security measures on individuals' privacy rights. The PIA process involves identifying the personal data that will be collected, processed, and stored, as well as the potential privacy risks

associated with these activities. Bodies can use this information to identify ways to mitigate privacy risks and ensure that cyber-security measures are in line with ethical principles and values. By conducting PIAs, organizations can proactively address privacy concerns and demonstrate a commitment to protecting individuals' privacy rights [Hernández-García Á., Kudenko D., 2022: 30]. Implementing transparency and accountability is an essential step for reconciling cyber-security and privacy concerns. Organizations can be transparent about their cyber-security practices by clearly communicating their data collection and processing practices to their customers. This includes providing clear and concise privacy policies, informing customers about data breaches, and providing mechanisms for individuals to access, correct, or delete their personal data. The organizations can take responsibility for any breaches that occur by implementing incident response plans and promptly notifying affected individuals. This can help build trust with customers and demonstrate a commitment to protecting personal data, which is crucial for reconciling cyber-security and privacy concerns [Liao Q., 2022: 1072].

Balancing under study requires organizations to adopt a holistic approach that takes into account both security and privacy concerns. This involves implementing strategies like data minimization, encryption, and privacy impact assessments, while fostering a culture of privacy and transparency. By doing so, organizations are able to protect sensitive information from cyber threats and data breaches, while respecting individuals' privacy rights. A comprehensive and balanced approach that incorporates ethical principles and values, such as fairness, transparency, and accountability, is key to reconciling cyber-security and privacy concerns [Rajić M., Filipović S., 2021: 1–16].

## Conclusion

The article highlights importance of balancing cyber-security and privacy and valuable insights into the legal and ethical considerations involved. For sure, there are still several questions that require more research to enhance understanding of this topic. One possible avenue for future research is to investigate the impact of emerging technologies, such as artificial intelligence and block-chain, on cyber-security and privacy. Another important area of research is to explore the potential benefits and drawbacks of data sharing and data protection mechanisms, and how they can be opti-

mized to strike a balance between cyber-security and privacy. Hence, more research is needed to examine the ethical considerations involved in the use of cyber-security measures, such as the use of surveillance technologies and their impact on individual privacy rights. These research directions can help policymakers and industry leaders to make informed decisions and develop appropriate regulations that balance the competing interests of cyber-security and privacy. In the digital age maintaining cyber-security and protecting sensitive information are crucial, but must be balanced against the fundamental right to privacy. This challenge requires a comprehensive and rationale approach that respects both privacy rights and the need for robust cyber-security. Bodies can implement various measures like data minimization, encryption, privacy impact assessments to protect personal data from cyber threats while respecting individual privacy rights. Moreover, bodies must take responsibility for any breaches occur and be transparent about their cyber-security practices to build trust with customers and demonstrate a commitment to protecting personal data.

Ethical and legal considerations must be taken into account in the development of digital technologies and their regulation to ensure that personal data is protected while also allowing for cyber-security measures.

To achieve the balance it is necessary for policymakers, business and individuals to collaborate and develop comprehensive solutions protecting sensitive information without infringing on individual privacy rights. This will require continuous education and awareness-raising initiatives to foster a culture of privacy and cyber-security. It will also require the development of legal frameworks that strike a balance between these two values. Prioritizing ethical and legal considerations in the development of digital technologies and their regulation will ensure that everyone can benefit from the digital age while also safeguarding individual privacy rights. Achieving this balance requires ongoing collaboration and dialogue between stakeholders to ensure all perspectives are considered and that the solutions implemented are sustainable and respectful of individual privacy rights.

On one hand, cyber-security is essential for protecting sensitive information and ensuring the proper functioning of digital systems. On the other hand, privacy is a fundamental human right that must be respected in any technological context.

A careful balance between these two values can be achieved through a combination of legal and technical measures, such as encryption, access

controls, and data minimization. It also emphasizes importance of international cooperation and coordination in addressing cyber-security and privacy concerns, as these issues are global in nature and require a collective response.

Cyber-security and privacy are two fundamental human rights that are often in conflict with each other. With increasing threat of cyber-attacks and data breaches, the need to maintain cyber-security and protect sensitive information has become more important than ever. However, in the process of implementing cyber-security measures, there is a risk of infringing on the right to privacy. The problem statement is that the current legal framework for cyber-security and privacy in various jurisdictions is inadequate in addressing the challenges of maintaining cyber-security while respecting privacy rights. The article emphasizes the need for a careful balance between cyber-security and privacy and suggests ways in which cyber-security and privacy concerns can be reconciled in a general context. By doing so, it aims to raise awareness of the need for ethical and legal considerations in the development of digital technologies and their regulation.

## References

1. Abdul-Kareem A. (2021) Judicial Review of Electronic Evidence in the UAE: Challenges and Solutions. *Computer Law & Security Review,* vol. 41, p. 105488. Available at: https://doi.org/10.1016/j.clsr.2021.105488

2. Acquisti A., Grossklags J. (2013) Economics and Privacy. *Journal* of *Economic Literature*, vol. 51, no. 2, pp. 1–32.

3. Al-Fadhli N. (2021) UAE Cybercrime Law: Vague and Broad? *Journal of Information Privacy and Security,* vol. 17, no. 1, pp. 18–25. Available at: https://doi.org/10.1080/15536548.2021.1878225

4. Axelsson A.-S., Söderberg J. (2022) Cybersecurity and Privacy: The Interplay between Individual Rights and Organisational Responsibilities. *Computer Law Security Review,* vol. 43, p. 105639. Available at: https://doi.org/10.1016/j.clsr.2022.105639

5. Bamberger K., Mulligan D. (2019) *Privacy on the Books and on the Ground.* Cambridge University Press.

6. Barnes D., Liang X. (2022) Privacy, Security, and Ethics in Information Systems. *Information and Management*, vol. 59, no. 1, p. 103598. Available at: https://doi.org/10.1016/j.im.2021.103598

7. Bergmann M., Grohmann B. (2022) Cyber-security, Discrimination, and Fairness: A Systematic Literature Review. *Journal* of *Business Re-*

*search*, no. 143, pp. 197–207. Available at: https://doi.org/10.1016/j.jbusres.2021.08.010

8. Brennan-Marquez K., Hoffman S. (2022) Fragmentation and the Future of Privacy Law. *Columbia Law Review*, vol. 122, no. 1, pp. 9–55. Available at: https://doi.org/10.2139/ssrn.3883466

9. Chakraborty R. (2021) Data Security and Privacy: The Need for a Comprehensive Cyber-Security Strategy. *Journal of Public Affairs,* p. 2727. Available at: https://doi.org/10.1002/pa.2727

10. Chia P., Teo T. (2021) Cyber-security and Privacy in Australia. *Computers & Security,* no. 105, p. 102307. Available at: https://doi.org/10.1016/j.cose.2021.102307

11. Choo K.-K., Tan H. (2021) Privacy and Security Challenges in a Connected World. In: K.-K. Choo (ed.). Cyber Security and Privacy. Cham: Springer, pp. 3–17. Available at: https://doi.org/10.1007/978-981-15-9029-9_1

12. Eubanks V. (2021) When Artificial Intelligence Systems Perpetuate Bias. *Communications* of *the ACM*, no. 2, pp. 22–25. doi: 10.1145/3442037

13. Fisher D. (2021) Cyber-security and Privacy Law: The Evolving Intersection. *Boston College Law Review*, vol. 62, no. 6, pp. 2129–2149. Available at: https://doi.org/10.2139/ssrn.3832595

14. Floridi L. (2021) The Ethics of Cyber-security, Privacy and Artificial Intelligence. *Philosophical Transactions of the Royal Society*, no. 379, p. 2020242. Available at: https://doi.org/10.1098/rsta.2020.0242

15. Floridi L., Taddeo M. (2016) What is Data Ethics? *Philosophical Transactions of the Royal Society,* no. 374, pp. 1-19. Available at: https://doi.org/10.1098/rsta.2016.0360

16. Ghosh D., Scott M. (2022) Data Protection and Cyber-security: Walking the Tightrope between Privacy and Security. *Computer Law & Security Review,* vol. 43, p. 105666. doi: Available at: https://doi.org/10.1016/j.clsr.2022.105666

17. Greenwald G. (2019) *Permanent Record*. N. Y.: Penguin.

18. Greenwald G. (2021) The National Security Agency in the Age of Cyber Surveillance. *Foreign Policy*, no. 237, pp. 78–86. Available at: https://doi.org/10.2307/26947126

19. Gross A., Acquisti A. (2021) Transparency and Control of Personal Data: Balancing Privacy and Security. *Computers & Security*, no. 105, p. 102260. Available at: https://doi.org/10.1016/j.cose.2021.102260

20. Gürses S., Troncoso C. (2022) Privacy and Security: Tensions and Synergies. *IEEE Security and Privacy*, vol. 20, no. 1, pp. 78–84. Available at: https://doi.org/10.1109/MSEC.2021.3104862

21. Hawkins D. (2022) Experts Weigh In: Can Security and Convenience Coexist in a Post-Pandemic World? Available at: https://www.security-

magazine.com/articles/96037-experts-weigh-in-can-security-and-convenience-coexist-in-a-post-pandemic-world

22. Hernández-García Á., Kudenko D. (2022) Security, Privacy and Ethics of Autonomous Systems: A Review. *Electronics*, vol. 11, no. 1, p. 30. Available at: https://doi.org/10.3390/electronics11010030

23. Hickman L., Martin C. (2022) The FTC's Unfulfilled Promise: Revisiting the Effectiveness of the FTC's Data Security Enforcement Program. *Ohio State Law Journal,* vol. 83, no.1, pp. 73–132. Available at: https://doi.org/10.2139/ssrn.3839553

24. Hirila-Rus A., Borza A. (2022) The Need for a Unified European Cyber-security Strategy. In: 2022 International Conference on Cyber-security and Privacy Engineering, pp. 1–6. Available at: https://doi.org/10.1109/CySEng.2022.00008

25. Hu M. (2021) The Need for Comprehensive Federal Privacy Legislation. *Harvard Journal of Law & Technology,* vol. 34, no. 2, pp. 501–534. Available at: https://doi.org/10.2139/ssrn.3537656

26. Ikram N., Burnett E. (2022) Data Minimization: a Key Tool in Managing Data Protection and Cybersecurity Risks. *Journal of Data Protection & Privacy,* vol. 6, no. 2, pp. 97–108. Available at: https://doi.org/10.1108/JDPP-01-2022-0003

27. Izumi K. (2021) Strengthening Japan's Data Protection Framework: An Analysis of Recent Developments. *Asian Journal of Law and Society,* vol. 8, no. 1, pp. 1–23. Available at: https://doi.org/10.1017/als.2020.29

28. Joo S. (2022) The Challenges of Data Privacy and Cyber-security in South Korea. *Business Law Today*, vol. 32, no. 3, pp. 23–27.

29. Kim M., Kim Y. (2021) A Study on Privacy Regulation in South Korea: Focusing on Personal Information Protection Act and Related Statutes. *Information Japan*, vol. 24, no. 5, pp. 2675–2692. Available at: https://doi.org/10.3390/info24050154

30. Kharraz A., Robertson W. et al. (2021) Cyber-security Investments: A Prioritization Framework. *IEEE Security & Privacy*, vol. 19, no. 3, pp. 13–23. Available at: https://doi.org/10.1109/MSEC.2021.3058652

31. Koops B., Newell B. et al. (2021) The EU General Data Protection Regulation: Implications for International Cyber-security. *Journal of Cyber-security*, vol. 7, pp. 1–19. doi:10.1093/cybsec/tyaa013

32. Koops B., Newell B. et al. (2021) Ethical Governance of Cyber-security Surveillance. *Ethics and Information Technology*, no. 2, pp. 93–109. Available at: https://doi.org/10.1007/s10676-021-09578-1

33. Kshetri N. (2021) Block-chain's Roles in Meeting Key Supply Chain Management Objectives. *International Journal of Information Management,* p. 102178.

34. Kshetri N. (2021) A Global Analysis of Data Breaches: Focus on Sensitive Data Theft. *Journal of Business Research,* no. 133, pp. 326–334. doi: 10.1016/j.jbusres.2021.01.032

35. Latham J., Sassenberg U. (2021) Managing Balance between Cyber-security and Privacy: A Review of Relevant Empirical Research. *Current Opinion in Psychology,* vol. 36, pp. 1–6. Available at: https://doi.org/10.1016/j.copsyc.2020.06.004

36. Leong K. (2021) The Cyber-security Act and the Personal Data Protection Act. *Computer Law & Security Review,* vol. 41, p. 105484. Available at: https://doi.org/10.1016/j.clsr.2021.105484

37. Liao Q. (2022) Translating the GDPR's Accountability Principle into Corporate Practice. *International Journal of Environmental Research and Public Heal*, vol. 4, p. 1072. Available at: https://doi.org/10.3390/ijerph19031072

38. Lips M., Stupar A. (2021). Cyber-security, Surveillance and Privacy: Ethical Issues in the COVID-19 Pandemic. *Journal of Information, Communication and Ethics in Society*, vol. 19, no. 1, pp. 60–75. Available at: https://doi.org/10.1108/JICES-10-2020-0122

39. Liu X. (2017) The Cybersecurity Law of the People's Republic of China: A Content Analysis. *International Journal of Cyber Criminology,* vol. 11, no. 1, pp. 1–20. Available at: https://doi.org/10.5281/zenodo.573584

40. López-Pozuelo J. et al. (2022) Machine Learning Bias in Cyber-security: A Systematic Review. *Future Generation Computer Systems,* no. 128, pp. 1146–1162. Available at: https://doi.org/10.1016/j.future.2022.09.019

41. Luiijf E., Douma A. (2019) Cyber Security and Resilience: What Are We Talking about? In: Cyber Security: From Technology to Society. Cham: Springer, pp. 3–14.

42. Mangla S. (2021) Cyber-security and Privacy: Balancing the Scales. *Journal of Cyber-security and Information Management,* no. 2, pp. 49–62. Available at: https://doi.org/10.21632/irjbs.12.1.1-16

43. Mendes R., Bonneau J. (2022) Balancing Privacy and Security: A Review of Technologies and Techniques. *IEEE Security & Privacy,* vol. 20, no. 2, pp. 78–89. doi: 10.1109/MSEC.2022.3125795

44. O' Harrow R. (2017) Privacy vs. Security: A False Dichotomy. *Journal of National Security Law & Policy,* vol. 9, no. 1, pp. 95–113.

45. Pavlou P., Lewis K. (2020) The Cambridge Handbook of Consumer Privacy. Cambridge: University Press.

46. Patterson M. (2021) The Weakening of Privacy Protection in Australia: A Critique of Recent Developments. *Melbourne University Law Review,* vol. 44, no. 3, pp. 825–857. Available at: https://doi.org/10.2139/ssrn.3759518

47. Purcell R. (2021) The GDPR: Success or Failure? *Journal of Data Protection & Privacy,* vol. 5, no. 2, pp. 135–148. doi: 10.1108/JDPP-12-2020-0053

48. Rajić M., Filipović S. (2021). Balancing Cyber-security and Privacy: An Ethical Perspective. *International Journal of Cyber-Security and Digital Forensics,* vol. 10, no. 1, pp. 1–16. Available at: https://doi.org/10.17781/P002959

49. Rass S. et al. (2021) Dealing with the Technical Complexity of Cyber-security and Privacy in the Digital Age. *Journal of Cyber-security*, no. 7, tyaa017. Available at: https://doi.org/10.1093/cybsec/tyaa017

50. Rosenzweig P. (2015) Balancing Privacy and Security: The Ethical Dimension. In: J. Quigley, D. Molnar (eds.) Routledge Handbook of Science, Technology, and Society. L: Routledge, pp. 318 –329.

51. Rideout V. (2022) Privacy in a Digital World: Canada's Laws Fall Short. *Canadian Journal of Law and Society,* vol. 37, no. 1, pp. 83–85. doi: 10.3138/cjls.37.1.83

52. Rizvi S., Alhadreti O. (2021) Investigating the Impact of Cyber-security Measures on User Experience. In: Proceedings of the 2021 3rd International Conference on Computing, Electronics and Communications Engineering, pp. 36–39. Available at: https://doi.org/10.1109/ICCECE52537.2021.9478139

53. Rosenberg Y. (2021) Creating a Culture of Privacy: Tips for Leaders. *Security Management*, no. 3, pp. 36–42. Available at: https://doi.org/10.1080/09540962.2021.1901422

54. Schaerer E. (2022) Cyber-security and Data Protection in Latin America: Regulatory Trends and Challenges. *Journal of Cyber Policy*, vol. 7, no.1, pp. 111–125. doi: 10.1080/23738871.2022.2040862

55. Singer N., Tufekci Z. (2021) The Ethics of Digital Contact Tracing. *Science*, no. 368, pp. 951–954. Available at: https://doi.org/10.1126/science.abb9414

56. Singer P., Tushman M. (2021) *Understanding Cyber-security and the Implications for National Security.* N. Y.: Columbia University Press.

57. Sharma R., Jindal A. (2022) Balancing Cyber-security and Privacy: A Review of the Literature. *Journal of Cyber-security*, vol. 8, no. 1, pp. 1–22. doi: 10.1093/cybsec/tyab006

58. Stevens A. (2022) Balancing Privacy and Cyber-security: A Delicate Dance. *Duke Law & Technology Review,* vol. 21, pp. 45–77.

59. Sun R., Xu Q. (2021) Innovate or Comply? Technology Adoption under the Chinese Regulatory Environment. *Information & Management*, vol. 58, no. 1, p. 103341. doi: 10.1016/j.im.2020.103341

60. Sundararajan M. (2022) Balancing Privacy and Cyber-security Using Encryption. *Journal of* Cyber-*security*, no. 81, tyac002. Available at: https://doi.org/10.1093/cybsec/tyac002

61.Taddeo M., Floridi L. (2021) The Challenges of Cyber-security and Privacy: A Review. *Science*, no. 371, pp. 53–54. doi: 10.1126/science.abf1424

62. Talbot D. (2021) The Cyber-Security-Privacy Paradox: Impact on Consumers, Businesses, and Governments. Available at: https://securityintelligence.com/posts/the-cybersecurity-privacy-paradox-impact-on-consumers-businesses-and-governments/

63. Thomas M. (2021) Data Protection: The UK's New Regime. *Computer Fraud & Security,* no. 3, pp. 6–9.

64. Van Eecke P., Oberschelp de Meneses A. (2021) The EU Cybersecurity Regime: GDPR and the NIS Directive Compared. *Journal of International Data Privacy Law,* vol. 11, no. 4, pp. 293–307. Available at: https://doi.org/10.1093/idpl/ipab015

65. Vadlamudi P. (2022) Balancing Cyber-security and Privacy: A Comprehensive Overview of Regulations, Challenges, and Solutions. *Journal of Information Privacy and Security,* vol. 18, no. 1, pp. 1–18. Available at: https://doi.org/10.1080/15536548.2022.2002224

66. Villeneuve E. (2022) The Privacy-Security Paradox: Navigating Ethical Tensions in the Age of Cyber-security. *Journal of Business Ethics,* vol. 183, no. 3, pp. 495–511. doi: 10.1007/s10551-019-04322-5

67. Warren M., Brandeis L. (1890) The Right to Privacy. *Harvard Law Review*, vol. 4, pp. 193–220. Available at: https://doi.org/10.2307/1321160

68. Wessel M., van der Sloot B. (2021) The US Needs Federal Privacy Legislation. *Journal of Cyber Policy,* vol. 6, no. 2, pp. 167–183. Available at: https://doi.org/10.1080/23738871.2021.1892145

69. White L. (2021) What Does Brexit Mean for GDPR? *Computer Fraud & Security,* no. 3, pp. 8–10. doi: 10.1016/S1361-3723(21)00043-5

70. Xu H., Zhang, R. (2021) Balancing Cyber-security and Privacy Protection. *IEEE Security and Privacy*, vol. 19, no. 2, pp. 9–12. Available at: https://doi.org/10.1109/MSP.2021.3055223

71. Yoo C. (2015) Cyber-security and Freedom on the Internet. *Harvard Journal of Law & Public Policy,* vol. 38, no. 1, pp. 129–137.

72. Zhang Y. (2021) The Legal Framework of China's Cyber-security: a Critical Review. *Journal of Cyber Policy*, vol. 6, no. 4, pp. 519–540. Available at: https://doi.org/10.1080/23738871.2021.1906843

73. Zheng Y. (2021) China's Cyber-security Law and its Implementation. *Telecommunications Policy*, no. 4, p. 102156. doi: 10.1016/j.telpol.2020.102156

**Information about the author:**

Naeem Allahrakha — LLM, Lecturer.

The paper was submitted to editorial office 11.06.2023; approved after reviewing 23.06.2023; accepted for publication 23.06.2023.