

UNIVERSITY OF TARTU
SCHOOL OF LAW

Claudia Järve

**Protection of human rights and personal data within e-Governments in
relation to good governance**

Master's thesis

Supervisor: Monika Mikiver, LL.M

Tallinn 2025

Table of contents

Introduction	2
1. The interplay between e-Governance and good governance	5
2. Human rights in e-Governments.....	11
2.1 The right to internet access	12
2.2 The right not to use the internet and non-discrimination.....	16
2.3 The right to privacy and data protection.....	21
3. Challenges in data protection in e-Governments	29
3.1 Violations in data protection.....	30
3.1.1 Data breaches.....	31
3.1.2 Mismanagement of health data.....	36
3.2 Cross-border data exchange.....	39
Summary	45
Resümee.....	48
Bibliography.....	51

Introduction

Technological advancements and innovations are fundamentally transforming various dimensions of human life, enhancing communication, fostering connectivity, and providing near-unlimited access to information. The delivery of services is evolving to be more efficient and convenient, including public services offered by governments. These advancements open up new ways to learn, entertain, work and explore beyond traditional boundaries of physical communities, geographical locations and social positions.¹ This is showcased with Europe's Digital Decade Programme 2030, a direction for digital transformation of the European Union by the year 2030 and establishes a framework for multi-country cooperation programmes.² Among many goals, it aims to empower 80% of the population with basic digital skills, to make key public services 100% online and provide every citizen access to their medical records online.³ Yet, the rise of these digital platforms raises important questions surrounding data privacy, security vulnerabilities, and the issue of digital divide.

In this landscape, the significance of data protection has intensified as governments have been enacting stricter privacy laws with the European Union's General Data Protection Regulation (GDPR) setting a global benchmark. Data protection by itself is topical for these reasons. While the GDPR has been inspiring regulations outside of the European Union, this thesis will be focused on the scope of the European Union. The topicality of this is displayed by the following. By the end of 2023, 65% of the world's population had their personal data covered under a data privacy regulation, compared to 10% in 2019.⁴ As consumers grow increasingly conscious of their data privacy, their desire for more control over personal information has surged.⁵ Moreover, they value the government's role in regulating the use of personal data.⁶ According to a 2024 report by Statista, 82% consumers in Europe said they are more likely to do business

¹ European Commission, 'Europe's Digital Decade' (EU Commission, 2025) <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade> accessed 28 April 2025.

² OECD, 'Digital Decade Policy Programme 2030' (OECD, 2023) <https://stip.oecd.org/stip/interactive-dashboards/policy-initiatives/2023%2Fdata%2FpolicyInitiatives%2F99995856> accessed 28 April 2025.

³ European Commission, 'Europe's Digital Decade: Digital Targets for 2030' (EU Commission, 2025) https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en accessed 28 April 2025.

⁴ Sara Ana Cemazar, '5 Most Important Data Protection Trends in 2024 and Beyond' (26 August 2021) Rocket.Chat <https://www.rocket.chat/blog/data-protection> accessed 28 April 2025.

⁵ Cisco, 'Consumer Privacy Survey' (November 2019) Cisco Cybersecurity Series https://iapp.org/media/pdf/resource_center/cisco_consumer_privacy_survey_nov2019.pdf accessed 28 April 2025, 4.

⁶ Ibid, 9.

with companies that are transparent about their data practices.⁷ Consequently, data protection has evolved from a mere technical or legal afterthought into a central concern for businesses, regulators, consumers and citizens.

This thesis will focus on the protection of personal data and human rights in the perspective of e-Governments, examining how the digital services they provide impact the protection of these rights. It aims to showcase the positive and negative effects of providing these services to citizens. The research questions guiding this thesis are whether e-Governments provide greater protection of human rights and personal data, particularly sensitive data like health data, when compared to traditional governments. Furthermore, it will assess whether human rights and personal data can be comprehensively safeguarded and explores effective strategies that governments can adopt to protect individual rights.

The objectives of this thesis are analyzing legal frameworks like EU regulations, directives, acts, as well as national laws derived from these regarding digitalization and data protection. It will also seek to uncover violations of data protection principles and relevant human rights, analyzing how e-Government policies and technologies contribute to the rise of such violations, encompassing data breaches, mismanagement of data, and possible discrimination.

The hypothesis of this thesis is that e-Governments are better equipped to protect human rights and personal data compared to traditional governments.

A methodology used in this thesis is the data gathering method, as the sources used in this thesis are mainly literature - from scholarly journal articles to relevant books discussing topics like digital development and e-Governance in the European Union - as well as case law from the Court of Justice of the European Union (CJEU), the European Court of Justice (ECJ) and national data protection authorities. The analysis of these sources will enable to formulate informed generalisations through inductive reasoning. The thesis will adopt a qualitative approach, focusing on theoretical examination of phenomena occurring in the Member States of Europe.

The first chapter of this thesis will dive into the concept and definition of e-governance and its relation to good governance, exploring what constitutes good governance, whether it is

⁷ Digital Samba, 'Data Privacy in 2025: Trends, Regulations, and Best Practices' (26 June 2024) <https://www.digitalsamba.com/blog/data-privacy-trends> accessed 28 April 2025.

interpreted universally, and how it relates to the safeguarding of human rights in e-Governments. The second chapter analyzes how tools and policies associated with e-governance affect the protection of human rights, such as the right to access the internet and the emerging right of the non-use of the internet. This will include a focus on the freedom of expression, freedom of information, and the right to non-discrimination, along with the EU distinctions between the right to privacy and data protection. These two chapters then follow up to the third chapter which discusses key challenges in data protection, especially regarding health data. The chapter will present case law that gives context to regulations established in the GDPR, including the right to access information and the right to erasure (right to be forgotten). Furthermore, it showcases challenges in cross-border data exchange and the protection of rights across Member States. Finally, the chapter analyzes violations in healthcare data management, with a particular focus on Estonia, which in the past year intensified its efforts in the area of health data processing and management.

Regarding previous research about e-Governance and data protection, the author of this thesis found that the research is often focused on the effects of the GDPR in national law or the security and technological advancements and challenges of e-Governance. There lacked academic work connecting e-Governance with good governance. Thus, this thesis aims to showcase the impact of e-Governance on human rights and data protection, focusing on the processing of personal data and the autonomy and non-discrimination of individuals within e-Governments.

Keywords: e-governance, good governance, data protection, human rights

1. The interplay between e-Governance and good governance

The term E-government makes reference to the use of Information and Communication Technologies (ICTs) by government agencies to improve their operations and service delivery.⁸ ICTs cover all technical means used to handle information and aid communication, from computer hardware to software.⁹ It is a broader term for Information Technology (IT), which refers to communication technologies like the internet, wireless networks, cell phones, computers, software, video-conferencing, and social networking, just to mention a few. Essentially covering all applications and services that enable users to access, retrieve, store, transmit, and manipulate information in a digital form.¹⁰ Essentially, ICTs facilitate access to, retrieval, storage, transmission, and manipulation of information in a digital context.

In the realm of governance, public value is a critical element that shapes government policies and decision-making processes. Throughout history, nations have grappled with the question of which governmental system is optimal, with democracy often hailed as the preferred structure. While currently the majority of the world claims and aims to be a democracy, we see oligarchy, for example, in the Russian Federation, and autocracy in North Korea and Eritrea. While e-governments do not constitute a specific political regime or system, they are fundamentally driven by the objective of promoting public value. Additionally, even though the term “electronic government” was first referenced with “electronic democracy” in 1992, e-government policies are not necessarily applied only in democratic States. Essentially, any State that uses the internet or has smart cards or biometric identification, even Bluetooth or CCTV, can be considered to apply e-government technologies. E-governments have become such an important aspect of our world in the realm of technology, international law, and State legislation that the United Nations has developed the E-Government Development Index (EGDI) that tracks the state of E-Government Development of the United Nations Member States.¹¹ This is

⁸ Jean Damascene Twizeyimana and Annika Andersson, 'The Public Value of E-Government – A Literature Review' (2019) 36(2) Government Information Quarterly 78-167, 167.

⁹ Eurostat, 'Glossary: Information and Communication Technology (ICT)' (Eurostat, 2023) [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_\(ICT\)](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_(ICT)) accessed 28 April 2025.

¹⁰ Food and Agriculture Organization of the United Nations (FAO), 'Information and Communication Technologies (ICT)' (FAO, 2025) <https://aims.fao.org/information-and-communication-technologies-ict> accessed 28 April 2025.

¹¹ United Nations Department of Economic and Social Affairs (UN DESA), 'E-Government Development Index (EGDI)' (UN DESA, 2025) <https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index> accessed 28 April 2025.

determined by the United Nations E-Government Survey, published by the Department of Economic and Social Affairs and prepared over two years.¹² So, for example, while democratic countries like Denmark, Estonia, Singapore, and the Republic of Korea are at the top 3 of the ranks for 2024, other forms of governments, like autocratic countries of the Kingdom of Saudi Arabia and the United Arab Emirates, are also to be found and not far behind, ranking both 6th and 11th respectively.¹³ Thus, e-Governance has surpassed being accompanied by “electronic democracy” and has developed into something that could possibly be applicable to any country, regardless of what form of traditional government the country upholds. However, even with various systems and forms of government, the focus on public welfare and efficiency is integral. Government actions need to provide policies, strategies, agendas, laws etc. for the good of its citizens. These policies need to be grounded in human rights standards and obligations.

Governance itself refers to all processes of governing.¹⁴ It means “the process of decision-making and the process by which decisions are implemented” and it can be used in many contexts, including international and national governance. The government is one of the actors in governance.¹⁵ “Good governance” is a relatively new term used for measuring how public institutions conduct public affairs, manage public resources, and guarantee the realisation of human rights.¹⁶ The Council of Europe introduced 12 Principles of Good Governance in its 2008 Strategy on Innovation and Good Governance at the Local Level. These are: 1) Democratic Participation; 2) Human Rights; 3) Rule of Law; 4) Public Ethics; 5) Accountability; 6) Openness and Transparency; 7) Efficient, Effective, and Sound Administration; 8) Leadership, Capability, and Capacity; 9) Responsiveness; 10) Sound Financial and Economic Management, 11) Sustainability and Long-Term Orientation and 12) Openness to Change and Innovation.¹⁷ However, as it is relatively new, there is no

¹² E-Estonia, 'Estonia is at the Top of the United Nations E-Government Ranking' (23 October 2024) <https://e-estonia.com/estonia-is-at-the-top-of-the-un-e-government-ranking/> accessed 28 April 2025.

¹³ United Nations Department of Economic and Social Affairs (UN DESA), 'E-Government Knowledgebase: Country Data' (UN DESA, 2025) <https://publicadministration.un.org/egovkb/Data-Center> accessed 28 April 2025.

¹⁴ United Nations Office of the High Commissioner for Human Rights (OHCHR), 'About Good Governance' (OHCHR, 2025) <https://www.ohchr.org/en/good-governance/about-good-governance> accessed 28 April 2025.

¹⁵ United Nations Economic and Social Commission for Asia and the Pacific (UN ESCAP), 'What is Good Governance?' (UN ESCAP, 2009) <https://www.unescap.org/sites/default/files/good-governance.pdf> accessed 28 April 2025.

¹⁶ n14

¹⁷ Council of Europe, '12 Principles of Good Democratic Governance' (Council of Europe, 2025) <https://www.coe.int/en/web/centre-of-expertise-for-multilevel-governance/12-principles> accessed 28 April 2025.

internationally agreed-upon definition of “good governance”,¹⁸ but there does seem to be overlapping attributes or characteristics identified with good governance. The UN Economic and Social Commission for Asia and the Pacific focuses on 8 major characteristics and states that good governance is 1) participatory; 2) consensus oriented; 3) transparent; 4) responsive; 5) effective; 6) equitable; 7) efficient and 8) follows the rule of the law.¹⁹ The Human Rights Council has identified 5 key attributes of good governance: 1) transparency; 2) responsibility; 3) accountability; 4) participation; and 5) responsiveness (to the needs of the people).²⁰ The overlaps and differences of these interpretations are illustrated below.

Council of Europe	EU Economic and Social Commission for Asia and the Pacific	Human Rights Council
Democratic Participation	Participatory	Participation
Human Rights	Equitable	
Rule of Law	Follows the rule of the law	Responsibility
Public Ethics	Consensus oriented	
Accountability		Accountability
Openness and Transparency	Transparent	Transparency
Efficient, Effective, and Sound Administration	Effective and efficient	
Leadership, Capability, and Capacity		
Responsiveness	Responsive	Responsiveness (to the needs of the people)
Sound Financial and Economic Management		

¹⁸ n14

¹⁹ n15

²⁰ n14

Sustainability and Long-Term Orientation		
Openness to Change and Innovation		

In general, the attributes and characteristics interpreted by these institutions remain, in part, similar to each other, and each of these has the intention of protecting human rights. However, good governance is an ideal, meaning that, by nature, it is challenging to achieve in its totality. E-governance seems to move towards this, however, with many of its policies and implementations providing progress in areas such as efficiency, transparency, public service delivery, accountability, responsiveness, etc. Many of which are considered to be attributes of good governance. This chapter analyzes whether e-governance provides protection of human rights from a good governance perspective.

In the realm of e-Governance, the once-only principle (OOP) has emerged as a concept aimed at reducing the administrative burden on citizens and businesses by minimizing their interaction with authorities. The goal is to enable public administrations to reuse data that has already been stored digitally, allowing citizens to provide information to the government only once.²¹ Automation and digitization of public services, such as electronic filing, digital signatures, or online applications reduce bureaucratic delays, accelerate processing times, minimize human error, and lower administrative costs.²² This enhances the efficiency and responsiveness attributes of good governance. Additionally, transparency and accountability are enhanced as e-Governance platforms enable real-time access to government information and decision-making processes, reducing opportunities for corruption. The digitization of services and public record allows citizens to monitor government activities and access policy documents, thereby enhancing institutional openness and building public trust.²³ Regarding accessibility, e-Government platforms allow individuals in remote or disadvantaged areas to access

²¹ Maarja Olesk, 'Challenges of Collaborative Digital Government: E-Participation, Open Government Data and Cross-Border Interoperability' (2020) Tallinn University of Technology <https://digikogu.taltech.ee/et/item/5325f102-b6c4-476e-885e-563cfe906cd9> accessed 28 April 2025, 42

²² Lazor et al., 'The Impact of E-Governance on Shortening the Public Service Delivery Terms' (2021) 26(3) Telos: Revista de Estudios Interdisciplinarios En Ciencias Sociales ,1133.

²³ Ibid, 1133, 1141; Andrianarivo Andriandafiarisoa Ralison Ny Avotra et. al 'Examining the Impact of E-Government on Corporate Social Responsibility Performance: The Mediating Effect of Mandatory Corporate Social Responsibility Policy, Corruption, and Information and Communication Technologies Development During the COVID era', 4.

government services independent of their location or physical ability.²⁴ Moreover, integration of e-Governance into the legal system, with the attention to privacy, security, and digital rights, fosters trust in government and ensures legitimacy and continuity of the rule of law²⁵, enhancing the rule of law attribute of good governance.

While this may work on a national level where governments can create their own systems and use their digital technologies to reduce interactions between government institutions and citizens, issues arise when trying to apply it on an international level, ensuring legal interoperability. While the OOP was introduced by the EU in its eGovernment Action Plan 2016-2020, the principle is defined and interpreted differently by the Member States. From a legal standpoint, the lack of clear legal obligation, the legal restrictions on data sharing, data protection, and confidentiality requirements, and the lack of legal validity of evidence have proved to be hurdles faced with cross-border OOP. Limitations arise with over-regulations, lack of digital literacy, or poor cyber security, which all can undermine e-Governance and good governance objectives.²⁶

Dr Katrin Merike Nyman-Metcalf, an Estonian-Swedish scholar, states in her article²⁷ that the legal issues surrounding e-governance do not form a single, unified area of law. She proposes that E-governance is often perceived as a highly technological and complex collection of technical requirements, and lawyers are often not involved until a later stage of the reforms. However, the most efficient and secure way to deal with the legal aspects of e-governance is not through complicated technical legislation, but by ensuring that e-services are integrated into the existing legal and administrative system of the country. This is an approach Estonia has adopted, with e-governance being an integral part of the legal and administrative system, and with as few special laws as possible.

Therefore, e-Governance is not a separate phenomenon, but rather an advanced stage in the evolution of good governance. Governmental bodies integrate ICTs to enhance their operational efficiency and service delivery, ultimately aimed at promoting public value. While traditionally associated with democratic regimes, e-governance has emerged as a versatile framework

²⁴ n22, 1134; Katrin Nyman Metcalf, 'How to Build E-Governance in a Digital Society: The Case of Estonia' (2019) 58 *Revista Catalana de Dret Públic* 1–12 <https://doi.org/10.2436/rcdp.i58.2019.3316> accessed 28 April 2025, 3.

²⁵ *Ibid*, 7.

²⁶ n22, 1134; n24, 7.

²⁷ n24, 7

applicable to various government forms, including autocracies. The United Nations' E-Government Development Index highlights the significance of these technologies across member states, showcasing that both democratic and non-democratic countries can leverage ICTs for effective governance. Moreover, governance itself encompasses the processes and decision-making mechanisms within public institutions. The principles of "good governance," as defined by various organizations, emphasize the importance of democratic participation, human rights, rule of law, transparency, accountability, and effective management of resources. Although there is no universally accepted definition, common themes emerge across different frameworks, aligning on the necessity for governance to be participatory, equitable, and responsive to the needs of citizens.

The integration of e-governance is not without challenges. Legal interoperability, data protection, digital literacy, and cybersecurity remain significant hurdles, particularly in cross-border contexts and in ensuring the protection of human rights. The Estonian model, which integrates e-governance into the existing legal and administrative framework with minimal special legislation, exemplifies a pragmatic approach to overcoming these obstacles and ensuring the continuity of the rule of law. The intersection of e-governance and good governance underscores the critical need for government actions to prioritize public welfare, efficiency, and adherence to human rights standards. While good governance remains an aspirational ideal, e-governance offers tangible mechanisms for progress by fostering participatory, equitable, and responsive public administration. As governments continue to navigate the complexities of the digital era, the principles of good governance, reinforced by innovative e-governance practices, will remain essential to ensuring that public institutions serve citizens effectively and uphold the foundational values of democracy and human rights.

2. Human rights in e-Governments

The thesis has thus far underscored the connection between e-Governance and good governance principles. It has been established that well-implemented e-Governance policies provide a direct reinforcement of certain basic attributes of good governance through a governmental framework that is considerably more transparent and efficient. In that framework, cases of wrongdoing or violations of policy are more easily visible, and the procedures of accountability are brought out and made readily accessible to the public.

While the establishment of good governance policies is important to enhancing the protection of human rights, other systems of rights that may remain less than adequately protected should also be considered. This includes relating the new rights arising in the context of the digital environment to rights that may not yet have been fully recognized, or from which a resort to protective measures does not yet enjoy clear consensus.

The primary objectives of this chapter are to offer a thorough examination of the relationship between the right to access the Internet and the right not to use it, while considering the implications of each option. Additionally, it will investigate whether these rights conflict with the right to non-discrimination. Furthermore, the chapter will explore the interaction between individual privacy rights and data protection rights, assessing whether they carry equal legal significance.

In addition, such an exploration will show how the characteristics most often associated with good governance in e-Government policies do not necessarily assure the protection of established anti-discriminatory rights. These differing rights, such as privacy, data protection, and access to the Internet, are interrelated and should be considered in conjunction when examining broader discourse on rights linked to e-Government initiatives. It is vital to assess how the use of technology in governments assists and at the same time obstructs the principles of good governance in e-Governments.

2.1 The right to internet access

The United Nations Human Rights Council formally recognized internet access as a human right in 2016, building upon earlier foundations that established the connection between the Internet, Information and Communication Technologies (ICTs), and human rights.²⁸ This recognition emerged from events such as the 2003 World Summit on Information Society (WSIS) and the 2005 Tunis Agenda, in which in paragraph 42 they state: “We reaffirm our commitment to the freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge. We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.”²⁹ From an international law standpoint, the Tunis Agenda is a consensus statement where the only requirement was not voicing a formal objection. It also connected the right to use the internet to Article 19 of the Universal Declaration of Human Rights,³⁰ which states: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”³¹ The right to use the internet became more and more topical during this time, with the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression submitting a report to the UN Human Rights Council in 2011 which makes 88 recommendations on the promotion and protection of the right to freedom of expression online. The report concluded that the internet is an “enabler” of other human rights and there should be little restriction to the flow of information via the internet.³²

This report affirmed the existing international human rights standards, especially Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which focus on the freedom of expression. In the European Union, the freedom

²⁸ Carolina Aguerre, 'Right of Access to the Internet - Global Approaches' in Human Rights, Digital Society and the Law (2025), 31.

²⁹ World Summit on the Information Society, 'Tunis Agenda for the Information Society' (18 November 2005) UN Doc WSIS-05/Tunis/Agenda <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html> accessed 28 April 2025.

³⁰ n28, 32.

³¹ Universal Declaration of Human Rights, UN General Assembly Resolution 217A (III), Art 19 (10 December 1948).

³² Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (16 May 2011) UN Doc A/HRC/17/27 <https://digitallibrary.un.org/record/706331?v=pdf> accessed 28 April 2025.

of expression is stated in Article 10 of the European Convention on Human Rights (ECHR). Access to the internet enables the exercise of freedom of expression, allowing individuals to speak, listen, share, and access information instantly across borders. It also provides a platform for marginalized groups, especially where traditional media are restricted or unavailable.³³

In 2016, 52 countries endorsed a draft resolution by the UN Human Rights Council in addition to Article 19 of the UDHR. It includes 15 recommendations and invokes the implications for three rights that are directly related to internet access, which are the freedom of expression, privacy and the right to education.³⁴ It also affirmed that human rights that people have offline must also be protected online.³⁵ The right to education is stated in Article 26 of the UDHR and Article 2 of the Protocol of the EDHR.

The Special Rapporteur underscored that Article 19 of the UDHR and the ICCPR was drafted “with the foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression. Hence, the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the internet.”³⁶ Any restrictions must meet a three-part test, the first part being legality (clear law), the second being legitimacy (serving purposes set out in article 19 paragraph 3 of the Covenant) and the third being necessity/proportionality (least restrictive means to achieve the purported aim).³⁷ The same rights people have offline must be protected online and Article 19 of both the UDHR and the ICCPR cover electronic and Internet-based modes of expression, safeguarding expression on the Internet in the same way as offline.³⁸

³³ n32, 7

³⁴ n28, 33

³⁵ UN Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (18 June–6 July 2018) UN Doc A/HRC/38/L.10/Rev.1 <https://documents.un.org/doc/undoc/ltd/g18/203/73/pdf/g1820373.pdf?OpenElement> accessed 28 April 2025.

³⁶ Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (16 May 2011) UN Doc A/HRC/17/27, Recommendation 21, 7 <https://digitallibrary.un.org/record/706331?v=pdf> accessed 28 April 2025.

³⁷ Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (16 May 2011) UN Doc A/HRC/17/27, Recommendation 24, 8 <https://digitallibrary.un.org/record/706331?v=pdf> accessed 28 April 2025.

³⁸ Miloon Kothari, 'The Sameness of Human Rights Online and Offline' in *Human Rights, Digital Society and the Law* (2025), 20.

The report of the Special Rapporteur also emphasized that several countries have already declared internet access as a human right, such as Estonia, which passed legislation in 2000 declaring internet access a basic human right, France, when the constitutional council of France declared internet access a fundamental right in 2009, and also Costa Rica, which reached a similar decision in 2010.³⁹ Additionally, the Special Rapporteur pointed out that a global poll the British Broadcasting Corporation (BBC) conducted with the international polling firm GlobeScan, concluded that 87% of 27 973 interviewees in 26 countries believe that internet access is a fundamental human right.⁴⁰ The poll also showed that while people considered it a fundamental right, they were still cautious about the dangers the internet brings, like possibly not being a safe place to express opinions, or worries about privacy and fraud.⁴¹

The role of governments regarding access to the Internet is promoting and facilitating access to the Internet, making it widely available and affordable, and ensuring that barriers (like technical, economic or regulatory) do not infringe on individuals' ability to exercise their expressive rights.⁴² This is considered a positive obligation. However, States may block, filter, or otherwise interfere with online content or access, which can seriously undermine freedom of expression and the right to information. While this is generally associated with authoritarian States like North Korea, which has heavily censored the access to the Internet, interference with access to the Internet also occurs in Europe, an area that is considered to have high levels of internet freedom. For example, Ukraine has restricted access to certain Russian websites and social media platforms as part of its measures during the ongoing conflict with Russia.⁴³ In 2023, Turkey blocked access to Twitter for a day following the criticism of the government's response to a 7.8-magnitude earthquake.⁴⁴ These are clearly violations of freedom of expression and access to information as the government is interfering with online content or access.

³⁹ Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (16 May 2011) UN Doc A/HRC/17/27, Recommendation 65, 18 <https://digitallibrary.un.org/record/706331?v=pdf> accessed 28 April 2025.

⁴⁰ BBC Press Office, 'Four in five regard internet access as fundamental right: global poll' (7 March 2010) https://www.bbc.co.uk/pressoffice/pressreleases/stories/2010/03_march/07/poll.shtml accessed 28 April 2025.

⁴¹ Ibid.

⁴² Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (16 May 2011) UN Doc A/HRC/17/27, Recommendation 5, 5 <https://digitallibrary.un.org/record/706331?v=pdf> accessed 28 April 2025.

⁴³ Paul Bischoff, 'Internet Censorship: A Map of Internet Censorship and Restrictions' (22 January 2025) Comparitech <https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/> accessed 28 April 2025.

⁴⁴ Robbie Mitchell, 'Tracking Internet Shutdowns in 2023' (11 January 2024) Internet Society Pulse <https://pulse.internetsociety.org/blog/tracking-internet-shutdowns-in-2023-2> accessed 28 April 2025.

Overall, the report of the UN Special Rapporteur and the draft resolution focused on the view that the internet is an enabler of other human rights and did not state that it is a human right in itself. The internet helps to exercise human rights such as the freedom of expression and the right to education, but also raises the issues of privacy.

Carolina Aguerre, an associate professor in the Department of Humanities and Communication at Universidad Católica del Uruguay, brought out threats and challenges of internet access in her chapter of the book *Human Rights, Digital Society and the Law*. She points out that technology innovation like mobile networks and phones have improved internet coverage, also to those in developing regions, but discrepancies remain essentially in infrastructure levels and digital capability building.⁴⁵ Besides infrastructural issues, internet access is also threatened by state and private sector actions such as content blocking, internet shutdowns, and filtering, which can undermine freedom of expression and restrict access for political, economic, or commercial reasons.⁴⁶

Carolina Aguerre also focuses on net neutrality, which is a central issue in internet governance and aims to ensure user's rights of access and sharing information with as little interference as possible.⁴⁷ According to Directorate-General for Communications Networks, Content and Technology of the European Commission, net neutrality is the principle that internet service providers (ISPs) treat all online traffic equally and openly, without discrimination, blocking throttling or prioritisation.⁴⁸ Net neutrality is considered a major achievement for the European Digital Single Market. However, she points out that regulatory frameworks are different across the globe, with concerns regarding zero-rating practices and discriminatory platform intervention, bringing forward examples like Latin America and Asia.⁴⁹

Thus, the recognition of internet access as a human right has evolved significantly within the framework of international law and human rights discourse. The United Nations Human Rights Council's 2016 resolution, building on foundational documents such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), affirms that the rights individuals enjoy offline, particularly freedom of

⁴⁵ n28, 35.

⁴⁶ Ibid, pp 35-36.

⁴⁷ Ibid, pp 36.

⁴⁸ EUR-Lex, 'Open Internet and Net Neutrality' https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=LEGISSUM:open_internet_and_net_neutrality accessed 28 April 2025.

⁴⁹ n28, 36

expression, must also be protected online. Article 19 of both the UDHR and ICCPR explicitly safeguards the right to seek, receive, and impart information through any media, including the internet, thereby establishing a clear legal basis for the protection of online expression.

Despite these advancements, significant challenges persist. Governments have a positive obligation to promote and facilitate affordable and widespread internet access, yet instances of state interference—such as content blocking, filtering, and internet shutdowns—continue to undermine freedom of expression and access to information. Notably, such practices are not confined to authoritarian regimes; even democratic states like Ukraine and Turkey have imposed restrictions in response to political or security concerns, raising critical questions about the proportionality and legitimacy of such measures. Ultimately, while the internet is not universally recognized as a human right in itself, it is widely acknowledged as an essential enabler of other fundamental rights, including freedom of expression, privacy, and education. The international community must therefore remain vigilant in upholding these rights online, ensuring that technological advancements serve to enhance, rather than restrict, the exercise of human rights in the digital age.

2.2 The right not to use the internet and non-discrimination

The right not to use the internet is a newer and less established concept. Traditional debates focus primarily on the right to access the Internet, framing it as an enabler of existing rights such as freedom of expression, access to information, and participation in public life, as analyzed in the previous subchapter. The right not to use the internet introduces the idea that digitization, while empowering and convenient, can become an obligation, especially when alternatives disappear or become impractical.⁵⁰ Comparing it to the right to internet access, which is recognized as an autonomous right, the right not to use the internet is often recognized as a derivative of other rights like privacy, equality and freedom.⁵¹ It seeks to protect individuals against the implicit or explicit obligation to be online, advocating for equal access to services

⁵⁰ Mart Susi, 'Framing the Right Not to Use the Internet' in *The Right Not to Use the Internet* (Routledge 2025), 47.

⁵¹ Ibid, 55.

via non-digital means. This right is also linked to freedom of choice⁵², non-discrimination, and human dignity.

Non-use of the Internet allows for greater control over personal data as the average user on the Internet leaves a trace.⁵³ While leaving a trace promotes transparency, which is an attribute of good governance, it takes away anonymity and privacy of the user. Someone who does not use the internet limits the possibility of anyone else having access to their personal data. Forcing digital-only engagement can undermine human dignity by reducing individuals' options for interaction, especially for those unable or unwilling to participate online due to economic, social, or personal reasons. The right not to use the internet is considered an aspect of the right to privacy and freedom of choice, protecting individuals from indirect discrimination and ensuring that non-digital alternatives remain available, particularly for those at risk of digital exclusion (e.g., the elderly, people with disabilities, low-income groups).⁵⁴ Thus, regulations requiring people to use digital means of communication with authorities might violate the fundamental right to equality and non-discrimination stated in Article 14 of the ECHR⁵⁵ and Article 2 and 7 of the UDHR.⁵⁶ Having access to public services only through the internet makes using the internet mandatory, which may compromise autonomy, privacy and personal data. Digital participation in governments should be voluntary and freedom of choice also encompasses the right to abstain from using digital networks. As the Internet is an ICT used by

⁵² Georgios Terzis, 'Ethical Meditations for a Human Right to an Analogue Life' in Dariusz Kloza, Elżbieta Kuźlewska, Eva Lievens, and Valerie Verdoodt (eds), *The Right Not to Use the Internet: Concept, Contexts, Consequences* (Routledge 2025), 21.

⁵³ Paolo Passaglia, 'An Attempt to Conceptualise the Right to Access the Internet and Its Impact on the Right Not to Use It' in Dariusz Kloza, Elżbieta Kuźlewska, Eva Lievens, and Valerie Verdoodt (eds), *The Right Not to Use the Internet: Concept, Contexts, Consequences* (Routledge 2025) 33.

⁵⁴ Elise Degrave, 'Digitalisation of Public Services in Belgium: Enshrining the Right Not to Use the Internet in the Constitution' in Dariusz Kloza, Elżbieta Kuźlewska, Eva Lievens, and Valerie Verdoodt (eds), *The Right Not to Use the Internet: Concept, Contexts, Consequences* (Routledge 2025), 180.

⁵⁵ EDHR Article 14: "The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status"

⁵⁶ UDHR Article 2: "The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status"; Article 7: "All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination."

e-Governments and digital public services are a core part of e-Governments, the question of compliance with non-discriminatory principles is raised.

Paolo Passaglia, a law professor at Università di Pisa, says that the non-use of the Internet is the result of omissions and inadequacies of the government's policies which are unable to overcome the digital divide.⁵⁷ He emphasizes the government's responsibility to facilitate the exercise of a right and asks the question of how the (social) right to access the Internet is put into practice. While there are mandatory exercises like compulsory education for minors, the decision to exercise some rights is left to personal discretion, for example the right to health.⁵⁸ This is also discussed in the health data protection chapter of this thesis, where it is highlighted how governments can set policies and put into force legislations to try and ensure the protection of health data, but the actual implementation of these policies and legislations is left to individuals who may either not be aware of the violations they carry out or violate norms intentionally.

Paolo Passaglia brings out in his chapter of the book '*The Right Not to Use the Internet*' that there are obstacles that hinder access to the Internet, such as economic gaps, cultural gaps, physiological gaps and geographical gaps. He says that these gaps arise from the unequal financial conditions of individuals, the different computer skills, the psychological handicaps of users, and disparities in Internet coverage in various territories.⁵⁹ The question of accessibility arises, another attribute of good governance, where people who lack the financial capabilities to buy a computer for example or live in an area where Internet access is not reachable or have inconsistent access to the Internet. In 2004, the Belgian Court of Arbitration addressed an issue where a law had replaced the official paper of legislation with online publication, making the Internet the only means to gain knowledge of the legislation. The Court emphasized that the challenged provisions made a significant number of people (those who were unable to access the Internet) "deprived of effective access to official texts".⁶⁰ The case is similar in Estonia, where Estonian legal acts are published only electronically in the Riigi Teataja (eRT).⁶¹ Riigi Teataja may be published on paper if online publication of legislation is

⁵⁷ n53, 36-37.

⁵⁸ n53, 36.

⁵⁹ Ibid, 35.

⁶⁰ Ibid, 37.

⁶¹ Riigi Teataja Act, § 7 (1): "The Riigi Teataja shall be available on the Internet free of charge."

impeded⁶² or when state authorities, nationwide associations of local authorities or legal persons in public law have ordered a consolidated text or a collection of consolidated texts⁶³. The last paper issue of Riigi Teataja was published in 2010.⁶⁴ Thus, as with Belgium, people who do not have access to the Internet in Estonia may not be aware of the legislations they have to follow.

The digital literacy gap also plays a significant role in the argument against the right of access to the internet. In 2023, 55% of people in the EU aged 16 to 74 had at least basic overall digital skills, ranging from 83% in the Netherlands to 28% in Romania.⁶⁵ According to the Digital Decade policy programme 2024 report of Estonia, 62,6% of the Estonian population has at least a basic level of digital skills.⁶⁶ One of the best performers other than the Netherlands in basic digital skills was Finland with 82% of its population having at least basic digital skills.⁶⁷ According to the Digital Inclusion Barometer, 40% of Belgians between the ages of 16 and 74 are digitally vulnerable.⁶⁸ According to statistics provided by an Eurostat survey, digital skills are heavily influenced by socio-demographic factors with only 28% of people aged 65-74 possessing at least basic digital skills.⁶⁹ Thus, having a basic right such as access to social housing, benefits and other public services are hindered by the fact that some people lack the digital literacy to actually benefit from the good governance attribute of efficiency in an e-government. Regarding this, it again raises the question of whether good governance attributes like efficiency and accessibility protect human rights such as the right to non-discrimination stated in Article 2 and 7 of the UDHR and Article 14 of the ECHR. This also goes against Chapter II para 2 of the “European Declaration on Digital Rights and Principles for the Digital Decade” where the European Parliament, the Council and the European Commission recalled

⁶² Riigi Teataja Act, § 11 (1): “If the online publication of the Riigi Teataja or online publication of legislation is impeded, the Riigi Teataja may be published on paper.”

⁶³ Ibid, § 11 (2): “The Riigi Teataja may be issued on paper as a special publication if state authorities, nationwide associations of local authorities or legal persons in public law have ordered a consolidated text or a collection of consolidated texts.”

⁶⁴ Riigikantselei, 'Täna ilmub viimane paberil perioodiline Riigi Teataja' (31 May 2010) <https://riigikantselei.ee/uudised/tana-ilmub-viimane-paberil-perioodiline-riigi-teataja> accessed 28 April 2025.

⁶⁵ Eurostat, 'Digital Skills in 2023: Impact of Education and Age' (22 February 2024) <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240222-1> accessed 28 April 2025.

⁶⁶ European Commission, 'Estonia 2024 Digital Decade Country Report' (9 July 2024) <https://digital-strategy.ec.europa.eu/en/factpages/estonia-2024-digital-decade-country-report> accessed 28 April 2025.

⁶⁷ European Commission 'Finland 2024 Digital Decade Country Report' (22 July 2024) <https://digital-strategy.ec.europa.eu/en/factpages/finland-2024-digital-decade-country-report> accessed 28 April 2025.

⁶⁸ King Baudouin Foundation, Digital Inclusion Barometer (2022) <https://digitall.be/situation-belgium> accessed 28 April 2025.

⁶⁹ Eurostat, 'Skills for the Digital Age' (April 2024) https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Skills_for_the_digital_age accessed 28 April 2025.

that “technology should be used to unite, and not divide, people”.⁷⁰ Therefore, making many public services available only through digital means could be considered discriminatory against people who lack this digital literacy, which are mainly the elderly.

Additionally, discrimination issues arise with accessibility for persons with disabilities, especially regarding relations with public services. Many government websites are only accessible with a mouse or a touch screen⁷¹, which in turn makes the websites inaccessible for people with cognitive or physical disabilities. The complexity of digital interfaces and the language used also present substantial barriers. Services rarely provide easy-read versions, audio descriptions, or simplified interfaces suitable for users with cognitive or intellectual disabilities. This lack of accessibility directly limits the autonomy of these individuals, often forcing them to rely on third parties and resulting in loss of privacy and independence.⁷²

This questions the conformity of semi-mandatory public services provided by e-Governments with Article 19 of the United Nations Convention on the Rights of Persons with Disabilities (CRPD)⁷³ and Article 26 of the Charter of Fundamental Rights of the European Union (CFR).⁷⁴ For example, the Belgian Constitutional Court found that moving official legal publications exclusively online deprived those unable to use the internet of effective access to the law, constituting discrimination.⁷⁵ This principle applies broadly: any digital-only public service risks excluding individuals who, by virtue of disability, age, economic situation, or lack of digital skills, cannot engage with these platforms. As rights need to be protected online and offline the same, international conventions bind States to promote accessibility not only in the environment, but also in ICTs, including e-Governance platforms. Article 9 of the CRPD

⁷⁰ European Commission, 'European Declaration on Digital Rights and Principles' (15 December 2022) <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles> accessed 28 April 2025.

⁷¹ n54, 175.

⁷² Sabrina Aouici, 'Is the dematerialisation of public services an elective progress? A sociological analysis of the (non)uses by older people in France', *The Right Not to Use the Internet: Concept, Contexts, Consequences* (Routledge 2025), 190.

⁷³ CRPD Article 19: “States Parties to the present Convention recognize the equal right of all persons with disabilities to live in the community, with choices equal to others, and shall take effective and appropriate measures to facilitate full enjoyment by persons with disabilities of this right and their full inclusion and participation in the community [...]”

⁷⁴ CFR Article 26: “The Union recognises and respects the right of persons with disabilities to benefit from measures designed to ensure their independence, social and occupational integration and participation in the life of the community”

⁷⁵ Pauline Lagasse and Sébastien Van Drooghenbroeck, 'Human rights and the digital divide: Recent developments in the case law of the Belgian Council of State' *The Right Not to Use the Internet: Concept, Contexts, Consequences* (Routledge 2025), 65

requires that both digital and non-digital channels remain genuinely available to ensure equal access.⁷⁶

Considering the above, the right not to use the Internet reveals a complex interplay between digital inclusion, human rights, and good governance. While digitization and e-Government initiatives can enhance efficiency and accessibility, they also risk marginalizing individuals who, due to economic, cultural, physiological, or geographical barriers, cannot or choose not to participate in the digital sphere. The Belgian and Estonian cases exemplify how exclusive reliance on digital platforms for official publications can deprive significant segments of the population—such as those lacking internet access or digital literacy—of their fundamental right to access the law. The digital literacy gap and the challenges faced by persons with disabilities raise concerns about indirect discrimination, affecting the compliancy of Articles 14 of the ECHR, Articles 2 and 7 of the UDHR, Article 19 of the CDPR and Article 26 of the CFR. Ultimately, the right not to use the Internet emerges as a necessary safeguard to ensure freedom of choice, privacy, and non-discrimination in an increasingly digital world. It calls for the preservation of non-digital alternatives and the proactive removal of barriers to both digital and analogue participation. As the text demonstrates, the responsibility lies with governments to bridge the digital divide and uphold the principles of equality and human dignity, ensuring that digital transformation does not come at the expense of fundamental rights.

2.3 The right to privacy and data protection

Making access to public services mainly digital affects the right to privacy, which is stated in Article 12 of the UDHR, Article 17 of the ICCPR and Article 8 of the ECHR. The right to privacy is also understood as a right to informational self-determination which means the right to control your own data by deciding what you share and how it is processed.⁷⁷ This includes protection of individuals from arbitrary or unlawful interference with privacy, family, home, or correspondence, including digital communications and data processed by e-Government systems. States are obligated to provide legal safeguards against such interference and ensure

⁷⁶ CRPD Article 9: “[...] States Parties shall take appropriate measures to ensure to persons with disabilities access, on an equal basis with others, to the physical environment, to transportation, to information and communications, including information and communications technologies and systems [...]”

⁷⁷ n54, 175.

that any restrictions on privacy are lawful, necessary, and proportionate to legitimate aims such as national security or public safety.⁷⁸

In the EU, data protection is recognized as a separate fundamental right in the Charter of Fundamental Rights of the European Union (CFR) under Article 8. The Charter separates the right to privacy (Article 7) from the right to data protection (Article 8). They are complementary rights protecting human dignity, but data protection principles evolved from privacy rights due to technological developments and is in itself broader and encompasses privacy. Data protection rights were mainly introduced with the GDPR, which is not considered a traditional human rights instrument.⁷⁹ Unlike traditional human rights, data protection rules already embody a compromise between individual rights and business interests, while the right to privacy protects the rights of the individual against governmental interference.⁸⁰ Recital 4 of the GDPR is worded as follows: “The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality”.⁸¹ Thus, data protection principles protect fundamental and non-fundamental interests, but data protection is not considered to be a traditional human right. Data protection principles establish principles such as data minimization, which states that you may only collect data that is necessary, purpose limitation, transparency and informed consent. Data protection is both an extension and a practical enforcement mechanism for privacy rights in e-Government settings.

Both the right to privacy and the right to data protection are legally enforced through principles such as data minimization, purpose limitation and transparency. With e-Governments, data exchanges happen between multiple government entities and sometimes in the private sector. Authorities should only collect data strictly needed for service delivery, a principle central to both privacy and data protection. However, digitalization of services often leads to more extensive data collection than offline alternatives, thus increasing the risk of intrusion into

⁷⁸ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, pp 14; General Assembly Resolution 68/167 (2013): The Right to Privacy in the Digital Age <https://digitallibrary.un.org/record/764407?v=pdf>, 2.

⁷⁹ Bart van der Sloot ‘Legal fundamentalism: is data protection really a fundamental right?’ *Data Protection and Privacy: (In)visibilities and Infrastructures*, 5

⁸⁰ Ibid, 16.

⁸¹ Recital 4, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [2016] OJ L 119/1.

private life.⁸² E-Governments should also implement mechanisms for individuals to give, withhold, monitor, and withdraw consent for the processing of their data.⁸³ For example, Estonia logs all access to citizens' data, allowing individuals to track who viewed their information and for what purpose.⁸⁴ This provides transparency, fostering accountability and protecting privacy and data protection rights.

As discussed previously, Article 8 of the Charter of Fundamental Rights of the European Union recognizes data protection as a separate right. The article also references the right of access and states that "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."⁸⁵ The GDPR further regulates this with Article 15, which states: "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed".⁸⁶ In Recital 63, this is further explained accordingly: "A data subject should have the right of access to personal data which have been collected concerning him, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing."⁸⁷ In the Case C-154/21, the Court (First Chamber) stated: "Article 15(1)(c) of GDPR must be interpreted as meaning that the data subject's right of access to the personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the actual identity of those recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) of GDPR, in which cases the controller may indicate to the data subject only the categories of recipient in question."

Article 15 of the GDPR establishes the right of access by the data subject. It gives individuals the right to obtain from a data controller confirmation on whether their personal data is being

⁸² n54, 174.

⁸³ Kevin Tammearu, 'What the United States Can Learn from Estonia on E-Governance' (31 August 2021) Center for European Policy Analysis <https://cepa.org/comprehensive-reports/what-the-united-states-can-learn-from-estonia-on-e-governance/> accessed 28 April 2025.

⁸⁴ n24, 9.

⁸⁵ Charter of Fundamental Rights of the European Union, [2012] OJ C 326/391. Art 8(2).

⁸⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) Art 15(1) [2016] OJ L 119/1.

⁸⁷ Recital 63, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [2016] OJ L 119/1.

processed, and if so, access to that personal data along with specific information about the processing. The controller must provide this information in a clear and accessible form, usually within one month of the request, and may provide the personal data copy electronically if requested. It is a prerequisite to exercising data subject rights such as rectification, erasure, restriction etc. This right is essential for the practical enforcement of data protection rights under the GDPR. It provides individuals with the tools to understand and oversee how their personal data is handled, thereby fostering trust and accountability in data processing practices across the European Union. When responding to an access request, the controller must provide detailed information about the processing, such as 1) the purposes of processing, 2) the categories of personal data processed, 3) the recipients or categories of recipients, 4) storage period, 5) data subject rights, 6) the right to lodge a complaint, 7) the envisaged period of data storage and 8) the existence of automated decision-making, including profiling.

The right to access is, however, also a "stand-alone" fundamental right, protected under Article 8(2) of the CFR. A data subject may just want to get information about the data processed about him or her - independent of the exercise of any other right under the GDPR. It also must also be balanced between the rights and freedoms of others, like trade secrets or copyright. Restrictions can also be based on unfounded or excessive requests or national or union law restrictions, i.e journalistic, scientific, statistical processing, or public interests.⁸⁸ The right of access is also a prerequisite for the exercise of other GDPR rights, such as rectification, erasure, or restriction of processing.

The CJEU has provided context to Article 15, for example in the case C-154/21⁸⁹, an individual in Austria had made a request to Österreichische Post AG for access to all personal data being stored (or previously stored) about him, specifically requesting information about the identity of any third parties to whom that data had been disclosed. Österreichische Post AG replied that it used personal data lawfully, but did not provide the specific identity of the recipients of the disclosed data, only general information. The individual then brought the proceedings before the Austrian courts, demanding Österreichische Post AG to give him the actual names of the recipients to whom his data had been disclosed. While Österreichische Post AG gave more

⁸⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [2016] OJ L 119/1. Art 15.

⁸⁹ Case C-154/21 RW v Österreichische Post AG [2023] ECLI:EU:C:2023:15. Found in <https://curia.europa.eu/juris/document/document.jsf?jsessionid=72A4296BAEB5A02A61313740EE3355EB?text=&docid=269146&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=15052991> accessed 28 April 2025.

details, it still did not name specific recipients. The court and appellate court both dismissed the claim, interpreting Article 15 of the GDPR as giving the data controller the option to inform the data subject, not obliging them. The Austrian Supreme Court referred the question of interpreting Article 15 of the GDPR to the CJEU. The CJEU concluded that the data controller must provide the actual identity of all recipients of personal data, but if the identity is unknown or the request is excessive/unfounded within the meaning of Article 12(5) of Regulation 2016/679 (GDPR), it may only provide categories of recipients in question.

In 2024, the German Chambers of Commerce and Industry (DIHK) conducted a survey among 4900 companies across almost all sectors. The survey deduced that 77% of companies that have difficulties responding to requests for access rights under Article 15 of the GDPR, have difficulties because there is legal uncertainty regarding the question of what is meant by the right to obtain a copy of personal data. 61% of those said that there is legal uncertainty regarding the question of when a request for access rights constitutes an abuse of law. These companies would also like to have more guidelines and recommendations that are practicable, clear and precisely worded. For example, the term “damages” is also unclear for these companies.⁹⁰ From this, it can be deduced that companies, while wanting the GDPR to be more simplified to not hamper innovation, they also want more specific guidelines and definitions, which could be contradictory.

Regarding the right of access and health data specifically, the case C-307/22⁹¹ involved a dispute between a patient and a healthcare practitioner regarding access to the patient's medical file. The patient received dental care from the healthcare practitioner, but suspected errors during the treatment. Because of this, the patient requested copies of their medical file, but the healthcare practitioner insisted that the patient must bear the costs associated with providing the copy. Initially, The individual's request for a free copy was granted, as the first-instance court based their interpretation of German national legislation in light of Article 12(5) and Article 15(1) and 15(3) GDPR. FT appealed this decision to the Bundesgerichtshof (Federal Court of Justice, Germany). The court stated that the solution to the dispute depends on the interpretation that should be given of the provisions of the GDPR. Therefore, the

⁹⁰ German Chamber of Commerce and Industry, 'Making Data Protection Practicable and Legally Certain' (2024) <https://www.dihk.de/resource/blob/115264/6ad66d3791681a2244f685810691e873/2024-dihk-umfrage-dsgvo-2023-en-bf-data.pdf> accessed 28 April 2025, 3, 7.

⁹¹ Case C-307/22 FT v DW [2023] ECLI:EU:C:2023:811. Found in <https://curia.europa.eu/juris/document/document.jsf?text=&docid=279125&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=14317229> accessed 28 April 2025.

Bundesgerichtshof referred the case to the CJEU as a preliminary reference. The CJEU held that the right to get a free copy of one's personal data is independent of the intent purpose for which the personal data is used and the controller must grant access.

The right to be forgotten is fundamentally connected to e-governance and (health) data protection through its function as a legal instrument empowering individuals to control (sensitive) personal information in the digital era. It is a principle stated in Article 17 of the GDPR and is a legal principle that allows individuals to request the removal of personal information about themselves from internet search results and other online directories. The core idea is that people should have the ability to control their digital footprint and not be perpetually stigmatized by past actions or information that is no longer relevant. Supporters of this right argue that it is essential for protecting privacy and combating harmful content, like revenge pornography. Critics find that it poses risks to transparency and public knowledge, especially concerning public figures and accountability. It can also be a gateway for politicians and criminals to erase negative aspects of their histories.⁹² A distinction should be made from the right to privacy. Instead, it balances privacy with freedom of information and expression.

In 2014, the *Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González* case set the legal precedent of the right to be forgotten. In this case, Costeja fell into debt, resulting in the Spanish government seizing his assets, auctioning his real estate and making announcements about the auction in the newspaper. When Costeja did a Google search of his name, links to the auction were among the first to appear. He turned to the newspaper, Google and the Agencia Española de Protección de Datos (AEPD), Spain's official body responsible for data protection. The AEPD ordered Google to remove any links to the announcements. Google sued, basing its argument on not being responsible for the content of the newspaper and the case not being under the jurisdiction of Spain's data protection laws as it is an American company. The European Court of Justice (ECJ) ruled in Costeja's favor, cementing the right to be forgotten as a legal right. This policy was later included in the GDPR.

Another CJEU judgment regarding the right to forgotten would be the *GC et al v. CNIL* case from 2019⁹³, which was a dispute between Google and the Commission nationale de

⁹² EBSCO, 'Right to Be Forgotten: Overview' (EBSCO Research Starters) <https://www.ebsco.com/research-starters/law/right-be-forgotten-overview> accessed 28 April 2025.

⁹³ Case C-136/17 *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECLI:EU:C:2019:773. Found in <https://curia.europa.eu/juris/document/document.jsf?jsessionid=1BD2DD3CF5E413E063C1046DD63>

l'informatique et des libertés (CNIL; French Data Protection Authority). In this case, four individuals asked Google to remove certain links from search results that appeared when searching their names. The links led to websites containing personal information they considered sensitive, inaccurate, outdated, or damaging, and that related to special categories of personal data or criminal convictions. Google refused these requests. After Google refused, the applicants complained to the French Data Protection Authority (CNIL) asking it to order Google to de-reference the links. CNIL also declined to take action. Then the applicants appealed CNIL's decision to the Conseil d'État (France's highest administrative court), which in turn referred several questions on the interpretation of EU data protection law to the Court of Justice of the European Union for a ruling. The key question was whether and under what circumstances operators of search engines like Google are obliged to grant requests to remove links from search results that relate to sensitive personal data and criminal convictions, particularly when the information is outdated, incomplete, or no longer corresponds to reality. The Court found that search engines must, in principle, remove links from search results in response to a legitimate request relating to special categories of data or criminal data, unless a compelling public interest justifies keeping the link visible. However, search engine de-referencing requests are limited to the EU domain, meaning Google has to only remove links from EU search results.

The right to be forgotten came up in the Clearview AI case⁹⁴ where the Commission nationale de l'informatique et des libertés (CNIL) aka the French Data Protection Authority received complaints from individuals about Clearview AI's facial recognition software and opened an investigation. On 26 November 2021, the Chair of the CNIL decided to give Clearview AI formal notice to cease the collection and use of data of persons on French territory in the absence of a legal basis to facilitate the exercise of individuals' rights and to comply with their requests for erasure. Clearview AI did not comply which resulted in The Chair of the CNIL therefore decided to refer the matter to the restricted committee, which is in charge for issuing sanctions. The restricted committee decided to impose a maximum financial penalty of 20 million euros.

[EA964?text=&docid=218106&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=13698958](https://eur-lex.europa.eu/eli/reg/2018/1725/oj/EA964?text=&docid=218106&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=13698958) accessed 28 April 2025.

⁹⁴ European Data Protection Board, 'The French SA fines Clearview AI EUR 20 million' (20 October 2022) https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en accessed 28 April 2025.

Thus, the right to be forgotten gives data subjects the ability to request that their data be erased and imposes data controllers the purposes and means of processing personal data. However, it is not absolute as data subject's rights need to be balanced against freedoms such as the right to information and freedom of expression. The regulation in the GDPR provides exceptions where erasure requests may be refused if continued processing is necessary to protect these competing interests. This balance should be considered by specific cases, analyzing the nature and sensitivity of the data, the interests of the public and also the role of the data subject in public life. The enforcement of the GDPR is left to national laws and supervisory authorities across EU Member States, taking into account context, proportionality, and legitimate competing rights.

The GDPR and related legal instruments have established a sophisticated and dynamic framework for the protection of personal data and privacy in the digital age. While significant progress has been made in clarifying and enforcing these rights, ongoing challenges, such as legal uncertainty and the need for clearer guidance, persist. The effective protection of personal data requires a continual balancing of individual rights, societal interests, and technological innovation, supported by vigilant oversight and adaptive legal interpretation. E-governance involves digitalization of public services, often relying on large-scale interoperable databases, with health records being among the most sensitive and integral data types managed by governments.

3. Challenges in data protection in e-Governments

Data protection is a critical aspect of e-government systems, as electronic data plays a central role in the functioning of digital systems. Insufficient data protection legislation may lead to the abuse of loopholes in data security. To ensure effective data protection, law and technology should work together, with technical solutions employed to protect data and the law requiring such solutions.⁹⁵ Moreover, data protection plays a critical role in e-government systems as it safeguards citizens' personal information and provides them with a sense of ownership of their data. To guarantee the privacy and security of personal data, certain measures must be implemented, including organizational, social, legal, and technical measures. Scholars from the data protection field, like Muhammad Hemin and Martin Hromada, emphasize the importance of enacting and enforcing data protection legislation, which can also support e-business efforts.⁹⁶ The government, as the responsible party in e-government initiatives, should establish information security objectives and allocate the necessary resources to achieve them.⁹⁷ Improving security procedures is essential to enhance security and privacy, as user privacy issues significantly impact the effectiveness of e-government.⁹⁸

It is necessary to discuss data protection legislation when talking about data exchange, as innovation in technology and its legislation are tightly connected when developing policies in an e-government. Legislations play a crucial role in improving citizens' trust in the services e-governments provide. In many countries, the majority of people still perceive that electronic data is more vulnerable than paper-based data, due to the new operations that can be performed, the enormous amounts of data that can be automatically processed, and the potential for personal information to be abused.⁹⁹ People will simply not use services that they do not trust.

With trust, there needs to be transparency and accountability, in addition to the enforcement of the law. Legal frameworks help create accountability and transparency in data handling. In Estonia, every query made by someone is recorded. This means you can easily check who has looked at your data, from general data to sensitive health data. Then, the person is entitled by

⁹⁵ n24, 9.

⁹⁶ Muhammad Hemin and Martin Hromada, "Evaluating a Proposed E-Government Stage Model in Terms of Personal Data Protection." (2023) *Applied Sciences* 13 (6), 2 <<https://www.mdpi.com/2076-3417/13/6/3913>> accessed 17 March 2025.

⁹⁷ n22, 1140.

⁹⁸ n96, 2.

⁹⁹ n24, 8.

law to ask the authority why they have looked at their data. The person can be confirmed because they use their ID card or other means of identification, as without it, there is no access provided.¹⁰⁰ This creates transparency, another good governance attribute, which is enhanced by e-government policies.

3.1 Violations in data protection

Health data is classified as one of the most delicate types of data and thus requires a higher level of protection. Additionally, processing health data needs to be handled with care as this sensitive data can be misused and result in a severe violation of privacy. Healthcare systems increasingly rely on digital technologies to manage and disseminate sensitive patient information, causing challenges associated with health data protection to become more prominent. This subchapter will analyze the obstacles that healthcare organizations face in safeguarding sensitive health data against unauthorized access, breaches, and other vulnerabilities. Understanding these challenges is crucial for developing effective solutions that ensure the protection of health data in contexts that rely heavily on e-Governments, such as Estonia.

There are certain key factors that contribute to the vulnerability of healthcare data, including human error, insufficient training, and the complexities of modern IT systems. Additionally, there is always the threat of external threats such as cyberattacks and data breaches, which have surged in frequency in recent years and impact data protection heavily. These threats not only compromise health data, but also undermine public trust in healthcare systems.

The Towards European Health Data Space (TEHDAS) project, co-funded by the EU's 3rd Health Programme, put together a report on secondary use of health data through European case studies. This report showed that across Europe, health data is being mismanaged by healthcare professionals. The report emphasized that poor data management procedures, lack of adherence to standards, excessive safeguards, poor data integration, lack of clear policies, misalignment across organizations, and loss of information all play a role in poor data management in

¹⁰⁰ n24, 9.

healthcare.¹⁰¹ As this thesis focuses on the interplay between e-Governance, human rights and data protection, this sub-chapter will focus mainly on issues pertaining to violations regarding mismanagement of health data based on the lack of adherence to regulations and the right to privacy and data protection.

3.1.1 Data breaches

A challenge that has grown more frequent in the recent years with digitalization is breaches of data, especially health data. Article 4 (12) of the GDPR states that a personal data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.¹⁰² Data breaches have become an increasingly alarming issue in recent years, with sensitive personal information being exposed and exploited on a global scale. Healthcare systems have been particularly vulnerable to data breaches, becoming victims of ransomware attacks. Violations of data protection laws, such as unauthorized access, processing, or disclosure of personal data, undermine data protection rights. While countries with high cybersecurity, like Estonia or Denmark, suffer from these attacks less, they still occur. Cybercriminals are getting smarter, the role of AI is increasing, possibly more and more cyberattacks will be political and thus an e-government can never be 100% safe.

Compliance with data protection regulations is supervised by independent supervisory authorities in each EU country. Data breaches can have severe consequences for individuals, including identity theft, fraud, and the misuse of sensitive personal information. Affected individuals may suffer both material and immaterial damages, and the potential for long-term identity theft issues can persist long after the initial breach. In case of a violation, these supervisory authorities may impose fines to the controller that can go as high as 4% of global annual turnover or 20 million euros.¹⁰³ Some of these fines will be discussed further into the sub-chapter.

¹⁰¹ TEHDAS, 'Report on Secondary Use of Health Data through European Case Studies' (28 February 2022) <https://tehdas.eu/app/uploads/2022/08/tehdas-report-on-secondary-use-of-health-data-through-european-case-studies-.pdf> accessed 28 April 2025, 24.

¹⁰² 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) [2016] OJ L 119/1.

¹⁰³ Matúš Mesarčík and Ondrej Hamulak 'General Data Protection Regulation: Current Challenges and Future Directions' *E-Governance in the European Union*, 129.

These breaches can also reduce trust in e-Governance and to fulfil the good governance attribute of participation as citizens need to use digital government services for e-Governments to be successful. When personal data is compromised, people lose confidence in the ability of organizations, including government institutions, to protect their information. The loss of privacy and confidentiality, as well as losing control over your personal information leaves an individual vulnerable and harbors distrust within the government and the application and enforcement of the rule of law. Thus, there is a reduced willingness in sharing data, which in turn hinders the growth of the participation attribute of good governance. As discussed in this thesis, participation should be voluntary and people should be able to choose whether to use services or not. The state is obliged to provide this comfortability and convenience if the aim is to provide good governance and protect rights like the right to privacy and data protection.

To mitigate this challenge, effective data protection must be provided to prevent unauthorized access and reduce the risk of violations. The technical measures controllers implement must be appropriate according to Article 34 (3)(a) of the GDPR.¹⁰⁴ Estonia uses X-Road and blockchain technology when processing data, enabling oversight and providing individuals with visibility over who accessed their data and why. These features help deter misuse and enable redress if violations occur. On the National Cyber Security Index, Estonia ranks 2nd, proving that Estonia is considered to be at the top regarding the protection of data. This is due to a multi-layered cybersecurity and data protection framework, consisting of legal frameworks like the Cybersecurity Act, the Estonian Information Security Standard (E-ITS) and compliance with the GDPR. The Information System Authority (RIA) handles cybersecurity and manages the technical platforms of Estonia.¹⁰⁵ However, even with high cybersecurity, Estonia has seen violations regarding data breaches, most notably the data leak in 2024 caused by a cyberattack at Allium UPI OÜ, which manages the loyalty programs of Apotheka pharmacies, Apotheka Beauty, and Petcity customer cards. The cyberattack resulted in leaking approximately 700,000 personal identification numbers, 400,000 email addresses, 60,000 home addresses, 30,000

¹⁰⁴ 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) [2016] OJ L 119/1 Article 34 (3)(a).

¹⁰⁵ Information System Authority, 'Tasks and Structure of the Authority' (Estonian Information System Authority, 3 January 2025) <https://www.ria.ee/en/authority-news-and-contact/authority-and-management/tasks-and-structure-authority> accessed 28 April 2025.

phone numbers and customers' purchase history.¹⁰⁶ In 2023, approximately 10,000 individuals' personal and health data were illegally downloaded from the testing company Asper Biogene. The breach involved genetic testing results, names, and personal identification numbers, affecting 40 healthcare companies. A criminal investigation was launched, and the AKI initiated a supervisory procedure.¹⁰⁷

Sweden, which also has a highly digitalized healthcare sector, has been experiencing an average of 662 cyberattacks per week against healthcare organizations as of late 2022 and early 2023. Notable incidents include temporary outages of the national eHealth portal (1177.se) and the sale of breached hospital data on the dark web.¹⁰⁸ Swedish hospitals have become among the most frequent targets of cyberattacks within the country, underlining the systemic risks posed by increasing digitalization.

In the U.K., three hospitals in Merseyside fell victim to a cyber attack when the personal details of 14,000 staff members were leaked via email in the Liverpool University Hospital Foundation Trust (LUHFT) Data Breach.¹⁰⁹ In France in 2022, Dedalus Biologie was fined €1.5 million for a massive breach affecting nearly 500,000 individuals and exposing sensitive information such as HIV status, cancers, genetic diseases, and pregnancies. More recently, in early 2024, Viamedis and Almerys, two main French healthcare service providers, suffered a breach affecting over 33 million people.¹¹⁰ Additionally, the vulnerability of healthcare management systems was highlighted when the Hipocrate Information System, which runs IT systems for

¹⁰⁶ Andmekaitse Inspektsioon, 'Möödunud Aastal Tehtud Rikkumistead | Andmekaitse Inspektsiooni Aastaraamat' (2024) <https://aastaraamat.aki.ee/aastaraamat-2024/moodunud-aastal-tehtud-rikkumistead> accessed 28 April 2025.

¹⁰⁷ ERR News, '10,000 people's data stolen in genetic testing company Asper Biogene leak' (1 April 2024) <https://news.err.ee/1609194952/10-000-people-s-data-stolen-in-genetic-testing-company-asper-biogene-leak> accessed 30 March 2025.

¹⁰⁸ Oskar Macgregor and Barbora Badurova, 'The ethics of choosing not to use the Internet: A comparative case study of the education and healthcare sectors in Slovakia and Sweden' *The Right Not to Use the Internet* (Routledge 2025), 211.

¹⁰⁹ 'Liverpool University Hospital Trust Data Breach.' <<https://www.hayesconnor.co.uk/group-actions/liverpool-university-hospital-foundation-trust-data-breach/>> accessed 27 March 2025; Bingham Long "LUHFT Data Leak Group Action Claim." (20 September 2023) <<https://binghamlong.co.uk/luhft-data-leak-group-action-claim/>> accessed 27 March 2025.

¹¹⁰ 'Health Data Breach: Dedalus Biologie Fined 1.5 Million Euros | European Data Protection Board.' <https://www.edpb.europa.eu/news/national-news/2022/health-data-breach-dedalus-biologie-fined-15-million-euros_en> accessed 27 March 2025; 'ISACA Now Blog 2024 Fallout from Viamedis Almerys Attack Does Not End with the Data Leak.' <<https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/fallout-from-viamedis-almerys-attack-does-not-end-with-the-data-leak>> accessed 27 March 2025.

many providers in Romania, was targeted by a ransomware attack in early 2024, directly affecting 25 hospitals and forcing 79 others to take their systems offline.¹¹¹

While these are only a few examples of attacks posed on hospitals or healthcare, the attacks against hospitals in general has seen a rising trend with ransomware attacks targeting hospitals and energy grids.¹¹² These attacks can not only harbor risks for data protection, but in general the risk to people's health as a study revealed that more than 20% of healthcare organizations experienced an increase in mortality rate after a significant cyberattack.¹¹³ These could range from life-threatening delays to treatment disruptions to diagnostic failures. An example for this would be the ransomware attack in Düsseldorf, where whilst enroute with a 78-year-old woman in a deteriorating state, paramedics were redirected to an alternative hospital 32 kilometres away due to systems being unavailable from the attack. The delay in treatment caused by the additional transfer time was initially suspected to have contributed to the patient's death, but was later found that the patient's condition was so severe the delay had no relevance to the final outcome.¹¹⁴ Therefore, these attacks could be issues of life and death.

Ransomware attacks on hospitals and healthcare systems have emerged as a significant concern, presenting serious risks to patient safety and operational integrity. During a critical meeting on November 8, 2024, the head of the United Nations health agency articulated that these cyber threats constitute a considerable challenge to international security.¹¹⁵ The Director-General of the World Health Organization (WHO) underscored the necessity for a unified government response, emphasizing that cybersecurity is a collective responsibility. He called for Member States to invest in advanced technology and to provide comprehensive training for personnel to effectively identify and respond to potential cyberattacks.¹¹⁶ The Head of the Delegation of the On the same date, the Head of the Delegation of the European Union to the United Nations

¹¹¹ Davey Winder, "Ransomware Attack Takes 100 Hospitals Offline." Forbes. <<https://www.forbes.com/sites/daveywinder/2024/02/13/ransomware-attack-takes-100-hospitals-offline/>> accessed 27 March 2025.

¹¹² Amit Singh 'From Past to Present: The Evolution of Data Breach Causes (2005–2025)' (March 24 2025), 1.

¹¹³ HIPAA Journal, 'Study Confirms Increase in Mortality Rate and Poorer Patient Outcomes After Cyberattacks' (2 October 2022) <https://www.hipaajournal.com/study-confirms-increase-in-mortality-rate-and-poorer-patient-outcomes-after-cyberattacks/> accessed 28 April 2025.

¹¹⁴ Stuart Kurutac, 'Understanding the Impact of Ransomware on Patient Outcomes – Do We Know Enough?' (16 June 2022) NCC Group <https://www.nccgroup.com/dk/research-blog/understanding-the-impact-of-ransomware-on-patient-outcomes-do-we-know-enough/> accessed 28 April 2025.

¹¹⁵ United Nations Security Council, 'Ransomware Attacks on Healthcare Sector "Pose a Direct and Systemic Risk to Global Public Health and Security", Executive Tells Security Council' (5 November 2024) <https://press.un.org/en/2024/sc15891.doc.htm> accessed 28 April 2025.

¹¹⁶ Ibid.

issued a statement addressing the alarming increase in ransomware incidents, predicting an attack frequency of every two seconds by the year 2031. He highlighted the EU's commitment to implementing robust measures to protect critical infrastructure and essential services, particularly within the healthcare sector. The EU's Network and Information Security Directive (NIS2), adopted in December 2022, sets out cybersecurity risk management and incident reporting requirements for critical sectors across the EU, and recognises health as a 'sector of high criticality'. These provisions are designed to enhance the cybersecurity posture of health facilities, safeguard sensitive medical data, and ensure the continuity of essential services amid persistent cyber threats.¹¹⁷ The effects of the countermeasures EU aims to provide is yet to be seen. However, timely countermeasures are critical to increase public trust in e-Governments, which is beneficial to both individuals and the public sector. Additionally, swift containment of an attack also reduces exposure to fines from the supervisory authority.

The research demonstrates that healthcare organizations are increasingly targeted by sophisticated ransomware attacks, with incidents in Estonia, Sweden, the United Kingdom, France, and Romania underscoring the global and systemic nature of the threat. In response, both international organizations and national authorities have recognized the urgent need for robust cybersecurity measures. The World Health Organization and the United Nations have emphasized that cybersecurity is a collective responsibility, requiring coordinated investment in technology, staff training, and proactive risk management. These regulatory frameworks, alongside the enforcement of the GDPR aim to safeguard personal data, ensure the continuity of essential services, and restore public confidence in digital governance. Nevertheless, the effectiveness of these countermeasures remains to be fully assessed, and the evolving nature of cyber threats means that absolute security may never be attainable. Therefore, ongoing vigilance, investment, and international cooperation are essential to mitigate risks, protect individual rights, and uphold the principles of good governance in the digital era.

¹¹⁷ 'EU Statement - UN Security Council: Briefing on Threats Posed by Ransomware Attacks against Hospitals and Other Healthcare Facilities' (8 November 2024) <https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-security-council-briefing-threats-posed-ransomware-attacks-against-hospitals-and-en?s=63> accessed 28 April 2025.

3.1.2 Mismanagement of health data

Regarding e-Governments, the policies introduce digital software systems which also include systems for health data management. These systems can vary between Member States, but also nationally within a Member State as well. The poor implementation of interoperability standards leads to difficulties in health data sharing, especially across borders. Additionally, the procedures differ among providers - while healthcare providers must adhere to the laws set in national law and the GDPR, they may each implement their own rules for data preservation and access, which could lead to fragmentation, duplication of effort, and reduced efficiency.¹¹⁸

One of the main issues with the mismanagement of health data in e-Governance is the over-anonymisation, overly cautious approaches, and lack of clarity on permissions and the application of the GDPR. The TEHDAS Report on secondary use of health data through European case studies showed that there is a lack of clarity on anonymisation processes on how to define the parameters for re-identification. Healthcare professionals may be overly cautious with processing data, considering all data as sensitive personal data out of fear of breaching privacy laws.¹¹⁹ Academic institutions also argue that pre-GDPR data cannot be reused as no consent was collected, which has led to difficulties obtaining individual-level data.¹²⁰

In Estonia, the Data Protection Inspectorate of the Republic of Estonia (AKI) focused on healthcare service providers (HSPs) in processing personal data in 2024. During that year, there were 184 cases of companies and institutions reporting to the AKI, which mostly related to the inattention, ignorance, or negligence of employees.¹²¹ For example, AKI revealed that every year there is a fairly large number of complaints from people who have discovered through the Health Portal data tracker that an unknown healthcare professional has viewed their data. These complaints divide into erroneous inquiries and curiosity enquiries.¹²² This brings out the other side of the coin, where healthcare service providers may know of the legislations, but can choose to ignore them anyway. And since access to sensitive personal data is simplified with digital systems, they may simply go forward with curiosity enquiries anyway. An example of a case where an employee carried out an erroneous or curiosity enquiry would be when an

¹¹⁸ n101, 23.

¹¹⁹ Ibid, 12.

¹²⁰ n118, 24-25.

¹²¹ n106.

¹²² 'Mis saab siis, kui arstid teevad uudishimupäringuid?' <<https://www.aki.ee/uudised/mis-saab-kui-arstid-teevad-uudishimuparinguid>> accessed 30 March 2025

employee of a private mental health clinic viewed the data of a patient who did not have a treatment relationship with them. Another similar example is the one coming from a large hospital where a hospital nurse viewed a patient's medical records 208 times in 13 months for personal purposes.¹²³ This unauthorized access to highly sensitive data not only shows an abuse of power, but also that the system is still vulnerable and it is not restricting access to this data enough. According to the GDPR and national laws of Estonia¹²⁴, a healthcare service provider may only make queries about a person's health data only if they have a legal basis for doing so. These legal bases are set in Article 6 of the GDPR, which stipulates conditions under which data may be processed, such as necessary for healthcare provision, public interest in public health, legal obligations and vital interests.¹²⁵ As health data is considered a special category of personal data according to Article 9 (1) of the GDPR¹²⁶, the processing of this sensitive data is more tightly regulated. The Article states that "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

The main legal basis is the existence of a treatment relationship. To mitigate this, the AKI directed more activities and training to healthcare service providers, where they explained the legal basis on when an HSP can process patient data in the health information system (the "Health Portal") without consent.¹²⁷ The AKI deduced that this knowledge, or lack thereof, was problematic. The GDPR places responsibility for data processing on the controller¹²⁸, thus also

¹²³ n106.

¹²⁴ Personal Data Protection Act (Estonia, 2019); Health Services Organisation Act (Estonia, 2008).

¹²⁵ 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) [2016] OJ L 119/1 Article 6 (1).

¹²⁶ 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) [2016] OJ L 119/1 Article 9 (1).

¹²⁷ Andmekaitse Inspektsioon, 'Tervishoiuteenuse Osutajate Kvaliteedimääruse Muudatused Isikuandmete Vaatest' (Andmekaitse Inspektsiooni Aastaraamat 2024) <https://aastaraamat.aki.ee/aastaraamat-2024/tervishoiuteenuse-osutajate-kvaliteedimaaruse-muudatused-isikuandmete-vaatest> accessed 30 March 2025.

¹²⁸ 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) [2016] OJ L 119/1 Article 24 (1): "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller

the obligation to implement technical and organisational measures to ensure sufficient data protection while processing.

While e-governments can implement more policies and heighten their cybersecurity level, the aspect of human error or curiosity can never be truly mitigated. A government body can never really regulate a) how a person acts, b) how malicious their actions are, c) if they have knowledge of the data protection violation they are carrying out, and if they do, will this knowledge be implemented? The principles and implementations of these principles must be taken into account when planning and implementing work arrangements affecting personal data, also considered integrated data protection. This means that, among other things, legal norms are implemented and technology is used by people. Therefore, even if everything is legally correct and procedures have been established in the organization and appropriate instructions have been created, they are of no use if employees do not implement them.¹²⁹

Taking all of the previously mentioned into account, it can be said that HSPs may not realize the amount of special types of personal data, health data that is entrusted to them, and what their obligations and responsibilities are when processing this data. They also may not realize that insecure information systems directly affect the lives and health of many people if their data falls into the wrong hands.¹³⁰ However, health professionals should know about the obligation to maintain patient confidentiality and the principles of medical ethics, as these are not recently developed concepts. A healthcare professional may make queries about a person's health data only if they have a legal basis for doing so. The main legal basis is the existence of a treatment relationship. While e-governments can implement more policies and heighten their cybersecurity level, the aspect of human error or curiosity can never be truly mitigated.

The AKI, with the research it gathered, understood that the data processing by HSPs needs to have more legal clarity and thus invited the Ministry of Social Affairs (SoM) to a joint discussion on how the provisions could be clarified. The SoM listened to the feedback of the AKI and the regulation of "Requirements for ensuring the quality of healthcare services and patient safety regulations" was amended on 01.11.2024, with adding a separate section that sets

shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary".

¹²⁹ Andmekaitse Inspektsioon, 'Miks on Vaja, Et Tervishoiuteenuse Osutajate Infosüsteemid Oleksid Turvalised?' <<https://aastaraamat.aki.ee/aastaraamat-2024/miks-vaja-et-tervishoiuteenuse-osutajate-infosusteemid-oleksid-turvalised>> accessed 18 March 2025.

¹³⁰ Ibid.

out the data processing principles for quality assessment, which are significantly clearer and oblige the healthcare service providers to define who, how and what data is collected, stored and used and how the privacy of persons using the services is ensured, following the applicable data protection standards.¹³¹ As this amendment was done in the previous year of this thesis, it is unclear whether this amendment has reduced the issue of curiosity inquiries done by HSPs in Estonia. What is clear is that a government body can never really regulate how a person acts, how malicious their actions are, if they have knowledge of the data protection violation they are carrying out and if they do, will this knowledge be implemented.

3.2 Cross-border data exchange

According to the Organisation for Economic Co-operation and Development (OECD), cross-border data flows are critical for global economic and social interactions as they support international business operations, logistics, supply chains and global communication.¹³² Cross-border data exchange in the EU refers to the transfer of personal and non-personal data across national borders within the EU and beyond, governed primarily by the GDPR and related EU laws to ensure consistent data protection standards. It enables healthcare professionals to securely access and share patients' key medical information across member states, improving the quality, continuity, and safety of care for citizens traveling or living abroad. The challenges with cross-border data flows are 1) privacy and data protection, 2) intellectual property, 3) digital security, 4) national security, 5) regulatory reach and 6) trade.¹³³ As discussed previously, fragmentation of the GDPR and legal standards in EU Member States result in legal uncertainty and variation in compliance regimes. This also applies to cross-border data exchange. Divergence in rules mean data controllers may face conflicting requirements when handling the same dataset across borders. Cross-border data processing is particularly illustrative in regards to health data processing as additional national rules regarding health and research data creates significant hurdles for cross-border health data sharing.¹³⁴ For example, Estonia's legal framework enables participation in cross-border health data exchanges, but slow

¹³¹ n127.

¹³² Organisation for Economic Co-operation and Development (OECD), 'Cross-border data flows' (OECD, 2024) <https://www.oecd.org/en/topics/cross-border-data-flows.html> accessed 28 April 2025.

¹³³ Ibid.

¹³⁴ n101.

integration remains due to discrepancies in judicial areas, divergent requirements for consent, and national-level conditions on data processing and retention.¹³⁵

The cross-border health data exchange in the EU is governed by a legal framework and governance structure, which encompasses both European and national legislation concerning data protection. At the core of this framework is the Directive 2011/24/EU, which establishes fundamental rights and guidelines for the processing of health data in the context of cross-border healthcare across EU borders, setting up interoperability and governance frameworks. Implementation of these guidelines is further clarified through the Commission Implementing Decision 2019/1765, which sets out the rules for network management and operational functionality. Additionally, special norms were introduced during the COVID-19 pandemic, reflected in Regulation 2021/953, to address emerging needs and challenges.¹³⁶

In 2025, the European Health Data Space Regulation (EDHS) was published and entered into force March 26th 2025. It aims to benefit all EU citizens, including patients, healthcare professionals, researchers, policymakers, and industry players.¹³⁷ It also amended Directive 2011/24/EU, mentioned previously, and Regulation 2024/2847 (The Cyber Resilience Act).¹³⁸ The EDHS aims to provide a trustworthy setting for secure access to and processing of wide range health data. It builds on existing horizontal EU frameworks, including the GDPR (Regulation 2016/679), the Data Governance Act (Regulation 2022/868), the Data Act (2023/2854) and the Network and Information Systems Directive (Regulation 2022/2555).¹³⁹ The EDHS seeks to establish a more consistent legal framework for secondary use of health data by defining specific roles like Health Data Holder, Health Data Access Body (HDAB) and Health Data User that align with the traditional Data Provider, Data-Sharing Intermediary (DSI) and Data User.¹⁴⁰ Scholars like Regina Becker and others say that the EDHS does not promote easy cross-border access to data. Each Health Data Access Body (HDAB) retains power over

¹³⁵ Kärt Salumaa-Lepik and Nele Sisu 'Data Protection Chapter' *Digital Development of the European Union: an interdisciplinary perspective*, 151.

¹³⁶ n135, 151.

¹³⁷ European Commission, 'My Rights Over My Health Data' (28 April 2025) https://health.ec.europa.eu/ehealth-digital-health-and-care/my-rights-over-my-health-data_en accessed 28 April 2025.

¹³⁸ Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 [2025] OJ L 2025/327.

¹³⁹ n137.

¹⁴⁰ Regina Becker et al., 'Legal bases for effective secondary use of health and genetic data in the EU: time for new legislative solutions to better harmonize data for cross-border sharing?' <https://academic.oup.com/idpl/article/14/3/223/7811298> accessed 28 April 2025, 237; n138.

access decisions for its Member State's data, often necessitating multiple reviews for a single cross-border request. This bureaucratic redundancy persists despite mechanisms for mutual recognition, due to differing ethical and legal concepts across Member States.¹⁴¹

Since this thesis mainly focuses on privacy and data protection, cross-border data exchange will be analysed in the realm of that. In 2019, the OECD Secretariat conducted a questionnaire and found that the main challenge regarding cross-border data flows was the uncertainty regarding legal privacy regimes.¹⁴² The uncertainty is highlighted in the survey results of the German Chambers of Commerce and Industry (DIHK), with the focus being on how data is transferred globally, including between Member States and third countries.¹⁴³

For transfers outside, the GDPR has set out mechanisms and safeguards to uphold an “essentially equivalent” level of protection, as brought out in the book chapter by Matúš Mesarčík and Ondrej Hamulak.¹⁴⁴ First are the adequacy decisions: the European Commission can decide that a third country ensures an adequate level of protection. This involves a legal assessment of the third country's laws, supervisory mechanisms, and international commitments. Transfers can occur freely from Member States to such countries. If there is no adequacy decision, transfers may be allowed if the data exporter implements appropriate contractual or organizational safeguards, such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), approved codes of conduct, or certification mechanisms. The exporting data controller is responsible for assessing the recipient country's legal environment to ensure effective protection.¹⁴⁵ Finally, if there is no adequacy decision nor proper safeguards, transfers can only proceed under narrowly defined exceptions, such as explicit consent, the performance of a contract, public interest, or protection of vital interests. These are intended to be used only when strictly necessary. Supervisory authorities have the power to prohibit data exports on grounds of inadequate protection.¹⁴⁶

The eHealth Digital Service Infrastructure (eHDSI) is an infrastructure ensuring the continuity of care for European citizens while they are travelling abroad in the EU. The two electronic cross-border health services currently being introduced in all EU countries are: 1)

¹⁴¹ n140, 240.

¹⁴² n132.

¹⁴³ n90, 4.

¹⁴⁴ n103, 126.

¹⁴⁵ Ibid, 128.

¹⁴⁶ Ibid, 128.

ePrescription/eDispensation and 2) Patient Summaries.¹⁴⁷ The Health Data Space Regulation (EHDS) mentioned before also introduced the HealthData@EU Central Platform, replacing the previous eHDSI¹⁴⁸ and enabling the secondary use of health data for research, innovation, policymaking, and public health. This HealthData@EU Central Platform release offers a set of reusable, open-source building blocks to support Member States in developing or connecting their national infrastructures to the EU-level platform. It aims to make health data exchange interoperable, secure, multilingual and user-friendly while ensuring clarity, reusability of data is built on existing open-source components.¹⁴⁹ It continues to provide the services of ePrescription/eDispensations and Patient Summaries.

Practical implementation of cross-border health data exchange has so far presented several challenges. Healthcare providers often require complete medical histories to ensure proper treatment, and having comprehensive access to information related to allergies and contraindications is critical, particularly in emergency scenarios where patients may be unable to provide such information themselves. This access significantly reduces the risks of medical errors that could arise from incomplete data. From a technical standpoint, the systems involved in cross-border health data exchange must be fully interoperable, compatible across various platforms, and secure and verifiable for effective use across borders. Importantly, data must be encrypted and protected during transmission, with private keys available solely to the designated contact points of Member States, ensuring that the Commission does not have access to patients' personal data. The EHDS aims to improve on this.

The EHDS regulates the primary and secondary use of health data. The primary use means using electronic health data to 1) treat or rehabilitate patients, 2) prescribe or dispense medical products and 3) deliver associated social, administrative, or reimbursement services. The secondary use refers to reusing existing data that was collected during primary use for scientific research purposes, public interest and policy support.¹⁵⁰ Under EHDS, individuals will be able to access and download a copy of health data, view access logs, set access restrictions and opt

¹⁴⁷ European Commission 'Electronic cross-border health services' (28 April 2025) https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en accessed 28 April 2025.

¹⁴⁸ European Commission, 'My Rights Over My Health Data' (28 April 2025) https://health.ec.europa.eu/ehealth-digital-health-and-care/my-rights-over-my-health-data_en accessed 28 April 2025.

¹⁴⁹ European Commission, 'European Commission Releases Open-Source HealthData@EU Central Platform — A Key Milestone for the European Health Data Space' (28 March 2025) <https://ec.europa.eu/newsroom/sante/newsletter-archives/61867> accessed 28 April 2025.

¹⁵⁰ n148.

out from data sharing where enabled, insert information into the Electronic Health Record, appoint an authorised individual to access the data and request rectification.¹⁵¹ The full implementation of the EHDS and with it the HealthData@EU Central Platform is planned over the next 10 years, with key parts of the Regulation entering into application in March 2029 in all EU Member States. In March 2034, third countries and international organisations will be able to join HealthData@EU for the secondary use. If the full implementation of this is successful, it would enhance healthcare service efficiency, generate savings, enable secure sharing of health data, give patients greater control of their health data and support cross-border collaboration.¹⁵² Therefore, the EDHS seems to comply with good governance attributes like transparency, accountability and responsibility with being able to view access logs. It also gives individuals access to their data and the option to download that data, thus being in compliance with Article 15 of the GDPR (right of access). However, as the EHDS and the HealthData@EU Central Platform are currently in their transitional period, the effects of them are yet to be seen.

Regarding the right to privacy and data protection, being able to opt out from data sharing and setting access restrictions gives individuals more protection in that regard as individuals could then be more in control of their data that is being processed. Thus, the management of health data within e-Government frameworks presents a complex interplay of technological, legal, and human factors. While digital software systems for health data management are increasingly prevalent across Member States, significant challenges persist due to inconsistent implementation of interoperability standards and divergent national procedures.

A central issue identified is the mismanagement of health data, often stemming from over-anonymisation, excessive caution, and a lack of clarity regarding permissions and the application of the GDPR. The Estonian case study provides concrete examples of the vulnerabilities inherent in digital health data systems. Despite the existence of robust legal frameworks, such as the GDPR and national laws, unauthorized access, whether through negligence, ignorance, or curiosity, remains a persistent problem. The AKI's efforts to address these issues through increased training and clarification of legal bases for data processing have been significant, yet the effectiveness of recent regulatory amendments remains to be seen.

¹⁵¹ Ibid.

¹⁵² European Commission, 'European Health Data Space Regulation (EHDS)' (28 April 2025) https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en accessed 28 April 2025.

While e-Governments can and should continue to refine policies, enhance cybersecurity, and clarify legal obligations, the human element, manifested in both error and intentional misconduct, cannot be entirely eliminated. As the GDPR stipulates, the responsibility for data protection lies with the controller, who must implement appropriate technical and organizational measures. These measures are only as effective as their implementation by individuals within the system. The recent regulatory amendments in Estonia, which aim to provide clearer data processing principles and assign explicit responsibilities to healthcare service providers, represent a positive step forward.

Summary

The thesis explored the dynamics between e-Governments, the protection of human rights and the safeguarding of personal data within the context of good governance in the European Union. The research has demonstrated that the digital transformation of public services, as exemplified by initiatives such as Europe's Digital Decade Programme 2030, has the potential to significantly enhance the efficiency, transparency, and accountability of government operations. By digitizing public services and leveraging advanced technologies, e-Governments can streamline administrative processes, mitigate bureaucratic barriers, and improve service accessibility for diverse populations. These improvements serve to reinforce the foundational principles of good governance, which are essential in fostering public trust and promoting civic engagement.

As advancements in technology continue to transform the delivery of public services, the importance of data protection has become increasingly prominent, primarily due to heightened consumer awareness and stringent regulatory frameworks, such as the GDPR. The findings demonstrated in this thesis show that when e-Governance is well-implemented, it can significantly reinforce attributes of good governance, such as transparency, efficiency, accountability, responsiveness, and rule of law, by digitizing public services and streamlining government-citizen interactions. The use of digital tools and automation in public service delivery reduces bureaucratic delays, minimizes errors, improves accessibility for diverse populations, and provides real-time access to information. This ultimately increases openness and public trust in government institutions, creating an environment where wrongdoing is more easily detected, and procedures of accountability are accessible to the public.

While e-Governments possess the potential to enhance these attributes, they simultaneously introduce new challenges related to privacy and security vulnerabilities. As government systems become more dependent on digital data, the risk and impact of data breaches, especially in sectors like healthcare, have grown significantly. As evidenced by recent data breaches, even countries with robust cybersecurity frameworks, such as Estonia, are not immune to violations that can undermine public trust and compromise individual rights. This undermines trust in e-Governance and could potentially leading to serious personal consequences such as identity theft and loss of privacy. Human error, insufficient training, poor implementation of standards, and inadequate policies contribute to frequent mismanagement of sensitive data, especially health data.

Furthermore, the analysis of cross-border data exchange has revealed significant legal and practical obstacles. The fragmentation of data protection regimes across EU Member States, coupled with divergent interpretations of the GDPR, creates legal uncertainty and complicates the seamless flow of information necessary for effective e-Governance. These challenges are particularly pronounced in the context of health data, where additional national regulations further hinder interoperability and the realization of a truly integrated digital single market. The methodology employed, which focused on a qualitative analysis of relevant literature and case law, facilitated an understanding of these phenomena across Member States.

The research questions guiding this thesis sought to assess whether e-Governments provide superior protection of human rights and personal data in comparison to a traditional government. Through an analysis of legal frameworks, the prevalence of data protection violations, and the implications of emerging technologies, this thesis posits that e-Governments are, in fact, better equipped to safeguard these rights, contingent upon the implementation of appropriate measures. The significance of transparent data practices was underscored by consumer sentiment, which highlights the necessity for governments to prioritize the protection of personal data. However, the mere existence of digital platforms does not automatically guarantee comprehensive protection.

The emergence of novel rights within the digital environment, such as the right to access or abstain from utilizing the internet, intersects with established rights including privacy, non-discrimination, and freedom of expression. These rights require careful consideration and integration within e-Government practices to ensure they are effectively safeguarded. Legislation like the GDPR set global standards and require governments to implement organizational, social, legal, and technological measures aimed at protecting personal data. Enforcement mechanisms, such as independent supervisory authorities and substantial fines for violations, serve to reinforce compliance and act as effective deterrents to potential infringements.

The findings of this research emphasize that while digital participation has the potential to empower citizens, this participation must remain voluntary to uphold autonomy, privacy, and choice. Governments bear the responsibility both to facilitate digital access and safeguard the right of individuals to opt out of digital engagement. This balance is essential to prevent exclusion

or coercion within the digitized public sphere. The voluntary nature of digital participation is essential to preserving individual autonomy and choice, and governments bear the responsibility to facilitate both access and non-use, thereby upholding the principles of non-discrimination and equality. Continuous improvement of legal clarity, interoperability standards, cybersecurity practices, and public awareness is required. Governments must remain vigilant and proactive in refining policy and practice to adapt to technological and societal shifts, thereby maintaining a balance between digital efficiency and the fundamental rights of individuals.

The newly introduced HealthData@EU Central Platform represents a significant step forward in establishing a cohesive framework for the utilization and exchange of electronic health data across the European Union. This platform is envisioned to facilitate a seamless integration of health data, thereby enhancing research capabilities, improving healthcare delivery, and ultimately benefiting patient outcomes across member states. As the European Health Data Space Regulation (EHDS) embarks on its transition period and the platform is not yet fully operational, there is a unique opportunity for scholarly research into the ramifications of this transitional phase on cross-border health data exchange. Research in this area could explore various dimensions, including the legal, technical, and ethical challenges that may arise as member states adapt to the new framework. Furthermore, understanding how the platform influences data-sharing practices and interoperability among nations could provide valuable insights into the effectiveness of the EHDS initiative. As the future unfolds, it is also crucial to consider the implications of this framework for data exchange not only within the EU but also with third countries. In the coming years, it is anticipated that non-EU countries and international organizations will be granted access to HealthData@EU for secondary use purposes, thereby expanding the scope of research opportunities and international collaborations.

In addition to examining cross-border data exchange, it is imperative to explore how the ongoing evolution of e-Governance strategies within various countries can intersect with the objectives of the HealthData@EU initiative. As multiple nations strive to enhance their e-Governance frameworks, there exists a ground for comparative research that analyzes the effectiveness, challenges, and best practices in health data governance across different jurisdictions. By delving deeper into these topics, scholars can contribute significantly to the understanding of how electronic health data can be harnessed to advance public health objectives and foster collaboration on an international scale.

Resümee

Käesolev magistritöö analüüsis e-Riigi, inimõiguste kaitse ja isikuandmete kaitse vahelist dünaamikat hea valitsemistava kontekstis Euroopa Liidus. Tehnoloogia arend mõjutav üha enam avalike teenuste osutamist, seega on andmekaitse tähtsus muutunud üha olulisemaks. Seda mõjutab peamiselt tarbijate teadlikkuse suurenemine ja ranged regulatiivsed raamistikud, nagu näiteks isikuandmete kaitse üldmäärus (IKÜT). Magistritöös esitatud tulemused näitavad, et kui e-Riik on hästi rakendatud, saab see tugevdada hea valitsemistava omadusi läbi avaliku teenuste digitaliseerimise ja valitsuse ning kodanike suhtluse sujuvamaks muutmise kaudu. Valitsemistava omadused, mida e-Riik potentsiaalselt tõhustab, on läbipaistvus, tõhusus, vastutus, reageerimisvõime ja õigusriik. Digitaalsete tööriistade ja automatiseerimise kasutamine avalike teenuste osutamisel vähendab bürokraatlikke viivitusi, minimeerib vigu, parandab juurdepääsu erinevatele elanikkonna rühmadele ja pakub reaajas juurdepääsu teabele, millele muidu oleks raskendatud juurdepääs. See suurendab lõppkokkuvõttes avatust ja usaldust valitsusasutuste vastu, luues keskkonna, kus isikuandmete kaitse rikkumisi on lihtsam tuvastada ja vastutuse protseduurid on avalikkusele kättesaadavad.

Kuigi e-Riigil on potentsiaal eelpool nimetatud hea valitsemistava omadusi parandada, toob e-Riik samal ajal kaasa uusi väljakutseid seoses privaatsuse ja turvalisusega. Kuna valitsussüsteemid muutuvad üha sõltuvamaks digitaalsetest andmetest, on andmelekete risk märkimisväärselt kasvanud, eriti sektorites nagu tervishoid. Sellised rikkumised võivad asetleida isegi riikides, kus on tugevad küberturvalisuse meetmed, õhnestades sellega usaldust e-Riigi vastu ja tuues kaasa tõsiseid isiklike tagajärgi nagu identiteedivargus ja privaatsuse kaotus. Inimlikud vead, ebapiisav koolitus, standardite halb rakendamine ja ebapiisav poliitika mõjutavad tundlike andmete väärjuhtimisele ja haldamisele.

Probleemid esinevad ka piiriüleses andmevahetuses ja ebajärjekindlus ning segased tõlgendused regulatsioonide ja aktide rakendamisel takistavad digitaalsete teenuste sujuvat kasutamist ja tekitavad õiguslikku ebakindlust nii kodanikele kui ka organisatsioonidele. Koostalitlusvõime puudumine ja standardite ebajärjekindel järgimine Euroopa liikmesriikides võivad viia killustatud poliitikani, ebatõhususeni ja andmekaitsepõhimõtete rikkumiseni. Kasutatud metoodika, mis keskendus asjakohase kirjanduse ja kohtupraktika kvalitatiivsele analüüsile, hõlbustas nende nähtuste mõistmist liikmesriikides.

Käesoleva magistritöö uurimisküsimused püüdsid hinnata, kas e-Riigid pakuvad inimõiguste ja isikuandmete paremat kaitset võrreldes traditsioonilise valitsusega. Õigusraamistike, andmekaitserikkumiste levimuse ja uute tehnoloogiate mõju aitas välja selgitada, et e-Riigid on paremini varustatud nende õiguste kaitsmiseks, kui rakendatakse asjakohaseid meetmeid. Läbipaistvate andmetavade olulisust rõhutas tarbijate arvamus, mis tõstis esile valitsuse vajadust seada isikuandmete kaitse esikohale. Digitaalsete platvormide olemasolu ei taga aga automaatselt igakülgset kaitset. Digitaalses keskkonnas tekivad uued õigused (näiteks õigus internetile juurde pääseda või sellest hoiduda), mis on seotud selliste kehtestatud õigustega nagu õigus privaatsusele, õigus mittediskrimineerimisele ja õigus sõnavabadusele. Need õigused vajavad hoolikat kaalumist ja integreerimist e-Riigi tavadesse, et tagada nende tõhus kaitse. Sellised regulatsioonid nagu IKÜT kehtestavad ülemaailmsed standardid ja nõuavad valitsustelt organisatsiooniliste, sotsiaalsete, õiguslike ja tehnoloogiliste meetmete rakendamist isikuandmete kaitseks. Sõltumatute järelevalveasutuste poolt jõustamine ja rikkumiste eest märkimisväärsede trahvide määramine tugevdab vastavust regulatsioonidele ja aktidele ning toimivad hoiatavate meetmetena.

Magistritöö rõhutab järeldusena, et kuigi digitaalne osalemine võib kodanikke võimestada, peab see jääma vabatahtlikuks, et säilitada autonoomia, privaatsus ja valikuvõimalused ning et sõnavabadus oleks kaitstud. Valitsustel on kohustus hõlbustada digitaalset juurdepääsu kui ka kaitsta õigust mitte kasutada digitaalseid võrke, ennetades seeläbi tõrjutust või sundi digitaliseeritud avalikus sfääris. Nii käesoleval hetkel kui ka tuleviku raames on vaja pidevalt parandada õiguslikku selgust, koostalitlusstandardeid, küberturvalisuse tavasid ja avalikkuse teadlikkust. Valitsused peavad jääma valvsaks ennetavaks poliitika ja tavade täiustamisel, et kohaneda tehnoloogiliste ja ühiskondlike muutustega, säilitades seeläbi tasakaalu digitaalse tõhususe ja üksikisikute põhiõiguste vahel.

Äsja kasutusele võetud HealthData@EU keskplatvorm on märkimisväärne samm edasi sidusa raamistiku loomisel elektrooniliste terviseandmete kasutamiseks ja vahetamiseks kogu Euroopa Liidus. See platvorm on ette nähtud terviseandmete sujuva integreerimise hõlbustamiseks, suurendades seeläbi teadusuuringute võimekust, parandades tervishoiuteenuste osutamist ja lõppkokkuvõttes parandades patsientide tulemusi kõigis liikmesriikides. Kuna see aga võeti alles hiljuti kasutusele, on see oma arengufaasis alles üleminekuperioodis. Sellega seonduvalt on võimalus edasiseks teaduslikuks uurimistööks selle üleminekufaaside mõjude kohta, eriti piiriülesele terviseandmete vahetamisele. Lisaks võiks platvormi mõju andmete jagamise tavadele ja riikidevahelisele koostalitlusvõimele anda väärtuslikku teavet EHDS-algatuse

tõhususe kohta. Tuleviku arenedes on oluline arvestada ka selle raamistiku mõjuga andmevahetusele mitte ainult ELis, vaid ka kolmandate riikidega. Lähiaastatel on oodata, et ELi mittekuuluvatele riikidele ja rahvusvahelistele organisatsioonidele antakse HealthData@EU-le juurdepääs teiseks kasutamise eesmärgil, laiendades seeläbi uurimisvõimaluste ja rahvusvahelise koostöö ulatust.

Lisaks piiriülese andmevahetuse uurimisele on hädavajalik uurida, kuidas e-valitsemise strateegiate pidev areng eri riikides saab olla kooskõlas HealthData@EU algatuse eesmärkidega. Kuna mitmed riigid püüavad oma e-valitsemise raamistikke täiustada, on olemas alus võrdlevaks uurimistööks, mis analüüsib terviseandmete haldamise tõhusust, väljakutseid ja parimaid tavasid eri jurisdiktsioonides. Nendesse teemadesse süvenedes on võimalik analüüsida, kuidas elektroonilisi terviseandmeid saab rakendada rahvatervise eesmärkide edendamiseks ja rahvusvahelise koostöö edendamiseks.

Bibliography

EU and Government Reports:

1. Council of Europe, '12 Principles of Good Democratic Governance' (Council of Europe, 2025) <https://www.coe.int/en/web/centre-of-expertise-for-multilevel-governance/12-principles> accessed 28 April 2025.
2. EUR-Lex, 'Open Internet and Net Neutrality' https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=LEGISSUM:open_internet_and_net_neutrality accessed 28 April 2025.
3. European Commission 'Electronic cross-border health services' (28 April 2025) https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en accessed 28 April 2025.
4. European Commission, 'Estonia 2024 Digital Decade Country Report' (9 July 2024) <https://digital-strategy.ec.europa.eu/en/factpages/estonia-2024-digital-decade-country-report> accessed 28 April 2025.
5. European Commission, 'Europe's Digital Decade' (28 April 2025) <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade> accessed 28 April 2025.
6. European Commission, 'Europe's Digital Decade: Digital Targets for 2030' (EU Commission, 2025) https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en accessed 28 April 2025.
7. European Commission, 'European Commission Releases Open-Source HealthData@EU Central Platform — A Key Milestone for the European Health Data Space' (28 March 2025) <https://ec.europa.eu/newsroom/sante/newsletter-archives/61867> accessed 28 April 2025.
8. European Commission, 'European Declaration on Digital Rights and Principles' (15 December 2022) <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles> accessed 28 April 2025.
9. European Commission, 'European Health Data Space Regulation (EHDS)' (28 April 2025) https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en accessed 28 April 2025.
10. European Commission 'Finland 2024 Digital Decade Country Report' (22 July 2024) <https://digital-strategy.ec.europa.eu/en/factpages/finland-2024-digital-decade-country-report> accessed 28 April 2025.

11. European Commission, 'My Rights Over My Health Data' (28 April 2025) https://health.ec.europa.eu/ehealth-digital-health-and-care/my-rights-over-my-health-data_en accessed 28 April 2025.
12. Eurostat, 'Digital Skills in 2023: Impact of Education and Age' (22 February 2024) <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240222-1> accessed 28 April 2025.
13. Eurostat, 'Glossary: Information and Communication Technology (ICT)' (Eurostat, 2023) [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information and communication technology \(ICT\)](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_(ICT)) accessed 28 April 2025.
14. Food and Agriculture Organization of the United Nations (FAO), 'Information and Communication Technologies (ICT)' (FAO, 2025) <https://aims.fao.org/information-and-communication-technologies-ict> accessed 28 April 2025.
15. OECD, 'Digital Decade Policy Programme 2030' (OECD, 2023) <https://stip.oecd.org/stip/interactive-dashboards/policy-initiatives/2023%2Fdata%2FpolicyInitiatives%2F99995856> accessed 28 April 2025.
16. Organisation for Economic Co-operation and Development (OECD), 'Cross-border data flows' (OECD, 2024) <https://www.oecd.org/en/topics/cross-border-data-flows.html> accessed 28 April 2025.
17. United Nations Department of Economic and Social Affairs (UN DESA), 'E-Government Development Index (EGDI)' (UN DESA, 2025) <https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index> accessed 28 April 2025.
18. United Nations Office of the High Commissioner for Human Rights (OHCHR), 'About Good Governance' (OHCHR, 2025) <https://www.ohchr.org/en/good-governance/about-good-governance> accessed 28 April 2025.

Books and Book Chapters:

19. Aguerre C, 'Right of Access to the Internet - Global Approaches' in Human Rights, Digital Society and the Law (2025).
20. Aouici S, 'Is the dematerialisation of public services an elective progress? A sociological analysis of the (non)uses by older people in France', The Right Not to Use the Internet: Concept, Contexts, Consequences (Routledge 2025).

21. Degrave E, 'Digitalisation of Public Services in Belgium: Enshrining the Right Not to Use the Internet in the Constitution' in Dariusz Kloza, Elżbieta Kuźelewska, Eva Lievens, and Valerie Verdoodt (eds), *The Right Not to Use the Internet: Concept, Contexts, Consequences* (Routledge 2025).
22. Kothari M, 'The Sameness of Human Rights Online and Offline' in *Human Rights, Digital Society and the Law* (2025).
23. Lagasse P and Van Drooghenbroeck S, 'Human rights and the digital divide: Recent developments in the case law of the Belgian Council of State' in *The Right Not to Use the Internet: Concept, Contexts, Consequences* (Routledge 2025).
24. Macgregor O and Badurova B, 'The Ethics of Choosing Not to Use the Internet: A Comparative Case Study of the Education and Healthcare Sectors in Slovakia and Sweden' in *The Right Not to Use the Internet* (Routledge, 2025).
25. Mesarčík M and Hamulak O, 'General Data Protection Regulation: Current Challenges and Future Directions' in *E-Governance in the European Union* (2024).
26. Passaglia P, 'An Attempt to Conceptualise the Right to Access the Internet and Its Impact on the Right Not to Use It' in Dariusz Kloza, Elżbieta Kuźelewska, Eva Lievens, and Valerie Verdoodt (eds), *The Right Not to Use the Internet: Concept, Contexts, Consequences* (Routledge 2025).
27. Salumaa-Lepik K and Sisu N 'Data Protection Chapter' in *Digital Development of the European Union: an interdisciplinary perspective* (2023).
28. Terzis G, 'Ethical Meditations for a Human Right to an Analogue Life' in Dariusz Kloza, Elżbieta Kuźelewska, Eva Lievens, and Valerie Verdoodt (eds), *The Right Not to Use the Internet: Concept, Contexts, Consequences* (Routledge 2025).
29. Susi M, 'Framing the Right Not to Use the Internet' in *The Right Not to Use the Internet* (Routledge 2025).
30. Van der Sloot B 'Legal fundamentalism: is data protection really a fundamental right?' in *Data Protection and Privacy: (In)visibilities and Infrastructures* (2017).

Articles and Journals:

31. Andrianarivo Andriandafiarisoa Ralison Ny Avotra et. al 'Examining the Impact of E-Government on Corporate Social Responsibility Performance: The Mediating Effect of Mandatory Corporate Social Responsibility Policy, Corruption, and Information and Communication Technologies Development During the COVID era'.

32. Jean Damascene Twizeyimana and Annika Andersson, 'The Public Value of E-Government – A Literature Review' (2019) 36(2) Government Information Quarterly 78-167.
33. Katrin Nyman Metcalf, 'How to Build E-Governance in a Digital Society: The Case of Estonia' (2019) 58 Revista Catalana de Dret Públic 1–12 <https://doi.org/10.2436/rcdp.i58.2019.3316> accessed 28 April 2025.
34. Lazor et al., 'The Impact of E-Governance on Shortening the Public Service Delivery Terms' (2021) 26(3) Telos: Revista de Estudios Interdisciplinarios En Ciencias Sociales.
35. Muhammad Hemin and Martin Hromada, "Evaluating a Proposed E-Government Stage Model in Terms of Personal Data Protection." (2023) Applied Sciences 13 (6), 2 <<https://www.mdpi.com/2076-3417/13/6/3913>> accessed 17 March 2025.
36. Regina Becker et al., 'Legal bases for effective secondary use of health and genetic data in the EU: time for new legislative solutions to better harmonize data for cross-border sharing?' <https://academic.oup.com/idpl/article/14/3/223/7811298> accessed 28 April 2025.
37. Twizeyimana, Jean Damascene, and Annika Andersson. 2019. "The Public Value of E-Government – A Literature Review." Government Information Quarterly 36 (2).

Web Pages and Blogs:

38. Andmekaitse Inspektsioon 'Miks on Vaja, Et Tervishoiuteenuse Osutajate Infosüsteemid Oleksid Turvalised?' <<https://aastaraamat.aki.ee/aastaraamat-2024/miks-vaja-et-tervishoiuteenuse-osutajate-infosusteemid-oleksid-turvalised>> accessed 18 March 2025.
39. Andmekaitse Inspektsioon, 'Mis saab siis, kui arstid teevad uudishimupäringuid?' (1 January 2024) <https://www.aki.ee/uudised/mis-saab-kui-arstid-teevad-uudishimuparinguid> accessed 30 March 2025.
40. Andmekaitse Inspektsioon, 'Möödunud Aastal Tehtud Rikkumistead' (2024) <https://aastaraamat.aki.ee/aastaraamat-2024/moodunud-aastal-tehtud-rikkumistead> accessed 28 April 2025.
41. Andmekaitse Inspektsioon, 'Tervishoiuteenuse Osutajate Kvaliteedimääruse Muudatused Isikuandmete Vaatest' (Andmekaitse Inspektsiooni Aastaraamat 2024) <https://aastaraamat.aki.ee/aastaraamat-2024/tervishoiuteenuse-osutajate-kvaliteedimaaruse-muudatused-isikuandmete-vaatest> accessed 30 March 2025.

42. BBC Press Office, 'Four in five regard internet access as fundamental right: global poll' (7 March 2010) https://www.bbc.co.uk/pressoffice/pressreleases/stories/2010/03_march/07/poll.shtml accessed 28 April 2025.
43. Bingham Long "LUHFT Data Leak Group Action Claim." (20 September 2023) <<https://binghamlong.co.uk/luhft-data-leak-group-action-claim/>> accessed 27 March 2025.
44. Davey Winder, "Ransomware Attack Takes 100 Hospitals Offline." Forbes. <<https://www.forbes.com/sites/daveywinder/2024/02/13/ransomware-attack-takes-100-hospitals-offline/>> accessed 27 March 2025.
45. Digital Samba, 'Data Privacy in 2025: Trends, Regulations, and Best Practices' (26 June 2024) <https://www.digitalsamba.com/blog/data-privacy-trends> accessed 28 April 2025.
46. E-Estonia, 'Estonia is at the Top of the United Nations E-Government Ranking' (23 October 2024) <https://e-estonia.com/estonia-is-at-the-top-of-the-un-e-government-ranking/> accessed 28 April 2025.
47. 'EU Statement - UN Security Council: Briefing on Threats Posed by Ransomware Attacks against Hospitals and Other Healthcare Facilities' (8 November 2024) <https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-security-council-briefing-threats-posed-ransomware-attacks-against-hospitals-and-en?s=63> accessed 28 April 2025.
48. European Data Protection Board, 'The French SA fines Clearview AI EUR 20 million' (20 October 2022) https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en accessed 28 April 2025.
49. ERR News, '10,000 people's data stolen in genetic testing company Asper Biogene leak' (1 April 2024) <https://news.err.ee/1609194952/10-000-people-s-data-stolen-in-genetic-testing-company-asper-biogene-leak> accessed 30 March 2025.
50. 'Health Data Breach: Dedalus Biologie Fined 1.5 Million Euros | European Data Protection Board.' <https://www.edpb.europa.eu/news/national-news/2022/health-data-breach-dedalus-biologie-fined-15-million-euros_en> accessed 27 March 2025
51. 'ISACA Now Blog 2024 Fallout from Viamedis Almerys Attack Does Not End with the Data Leak.' <<https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/fallout-from-viamedis-almerys-attack-does-not-end-with-the-data-leak>> accessed 27 March 2025.
52. HIPAA Journal, 'Study Confirms Increase in Mortality Rate and Poorer Patient Outcomes After Cyberattacks' (2 October 2022) <https://www.hipaajournal.com/study->

- [confirms-increase-in-mortality-rate-and-poorer-patient-outcomes-after-cyberattacks/](#) accessed 28 April 2025.
53. King Baudouin Foundation, Digital Inclusion Barometer (2022) <https://digitall.be/situation-belgium> accessed 28 April 2025.
54. Kevin Tammearu, 'What the United States Can Learn from Estonia on E-Governance' (31 August 2021) Center for European Policy Analysis <https://cepa.org/comprehensive-reports/what-the-united-states-can-learn-from-estonia-on-e-governance/> accessed 28 April 2025.
55. 'Liverpool University Hospital Trust Data Breach.' <<https://www.hayesconnor.co.uk/group-actions/liverpool-university-hospital-foundation-trust-data-breach/>> accessed 27 March 2025.
56. Paul Bischoff, 'Internet Censorship: A Map of Internet Censorship and Restrictions' (22 January 2025) Comparitech <https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/> accessed 28 April 2025.
57. Riigikantselei, 'Täna ilmub viimane paberil perioodiline Riigi Teataja' (31 May 2010) <https://riigikantselei.ee/uudised/tana-ilmub-viimane-paberil-perioodiline-riigi-teataja> accessed 28 April 2025.
58. Robbie Mitchell 'Tracking Internet Shutdowns in 2023' (January 11 2024) <https://pulse.internetsociety.org/blog/tracking-internet-shutdowns-in-2023-2>
59. Sara Ana Cemazar, '5 Most Important Data Protection Trends in 2024 and Beyond' (26 August 2021) Rocket.Chat <https://www.rocket.chat/blog/data-protection> accessed 28 April 2025.
60. Stuart Kurutac 'Understanding the Impact of Ransomware on Patient Outcomes - Do We Know Enough?' (June 16 2022) <https://www.nccgroup.com/dk/research-blog/understanding-the-impact-of-ransomware-on-patient-outcomes-do-we-know-enough/>
61. World Summit on the Information Society, 'Tunis Agenda for the Information Society' (18 November 2005) UN Doc WSIS-05/Tunis/Agenda <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html> accessed 28 April 2025.

Legal Documents:

62. Universal Declaration of Human Rights, UN General Assembly Resolution 217A (III), (10 December 1948).

63. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [2016] OJ L 119/1.
64. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 [2025] OJ L 2025/327.
65. Charter of Fundamental Rights of the European Union, [2012] OJ C 326/391.
66. Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (16 May 2011) UN Doc A/HRC/17/27, Recommendation 21, 7 <https://digitallibrary.un.org/record/706331?v=pdf> accessed 28 April 2025.
67. Personal Data Protection Act (RT I 2003, 26, 127).
68. Health Services Organisation Act (RT I 2001, 57, 358).
69. Riigi Teataja Act (RT I 2003, 26, 167).
70. Requirements for Ensuring the Quality of Healthcare Services and Patient Safety Regulations (RT I 2011, 18, 105).

Reports and Studies:

71. Cisco, 'Consumer Privacy Survey' (November 2019) Cisco Cybersecurity Series https://iapp.org/media/pdf/resource_center/cisco_consumer_privacy_survey_nov2019.pdf accessed 28 April 2025, 4.
72. EBSCO, 'Right to Be Forgotten: Overview' (EBSCO Research Starters) <https://www.ebsco.com/research-starters/law/right-be-forgotten-overview> accessed 28 April 2025.
73. German Chamber of Commerce and Industry, 'Making Data Protection Practicable and Legally Certain' (2024) <https://www.dihk.de/resource/blob/115264/6ad66d380d7ac209510d0fffd94613e3/german-digitalization-report-2024-pdf-data.pdf> accessed 28 April 2025.
74. Olesk M, 'Challenges of Collaborative Digital Government: E-Participation, Open Government Data and Cross-Border Interoperability' (2020) Tallinn University of Technology <https://digikogu.taltech.ee/et/item/5325f102-b6c4-476e-885e-563cfe906cd9> accessed 28 April 2025.

75. Singh A. 'From Past to Present: The Evolution of Data Breach Causes (2005–2025)' (March 24 2025).
76. TEHDAS, 'Report on Secondary Use of Health Data through European Case Studies' (28 February 2022) <https://tehdas.eu/app/uploads/2022/08/tehdas-report-on-secondary-use-of-health-data-through-european-case-studies-.pdf> accessed 28 April 2025.

Case law

77. Case C-136/17 GC and Others v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:773. Found in <https://curia.europa.eu/juris/document/document.jsf?jsessionid=1BD2DD3CF5E413E063C1046DD63EA964?text=&docid=218106&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=13698958> accessed 28 April 2025.
78. Case C-154/21 RW v Österreichische Post AG [2023] ECLI:EU:C:2023:15. Found in <https://curia.europa.eu/juris/document/document.jsf?jsessionid=72A4296BAEB5A02A61313740EE3355EB?text=&docid=269146&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=15052991> accessed 28 April 2025.
79. Case C-307/22 FT v DW [2023] ECLI:EU:C:2023:811. Found in <https://curia.europa.eu/juris/document/document.jsf?text=&docid=279125&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=14317229> accessed 28 April 2025.