MEDICINE, LAW & SOCIETY
Vol. 17, No. 1, pp. 89–108, April 2024

THE RIGHT TO PRIVACY AND DATA PROTECTION IN EUROPEAN HEALTHCARE SYSTEMS WITH AN EMPHASIS ON THE RELEVANT CASE LAW AND EUROPEAN LEGISLATION

Accepted
11. 12. 2023

Revised
2. 3. 2024

Published
18. 4. 2024

EMA TURNŠEK
University of Maribor, Faculty of Law, Maribor, Slovenia
ema@turnsek.com

CORRESPONDING AUTHOR
ema@turnsek.com

Abstract Are personal data and information, which we trust entirely to healthcare systems, sufficiently protected? The article deals with the crossroads of law and medicine, specifically at the point where the right to data protection of a patient is being breached or insufficiently protected by law. In this regard, we have to first learn what is the actual scope of person's right to (medical) data protection and second, understand when is that breached. The article analyses the origin of data protection and its historical development to find its core meaning. Further, it seeks the limits of data protection's scope with the content of other related rights. With a comprehensive overview of European case law, the article exposes some serious violations of individual's right to (medical) data protection.

Keywords
right to dignity,
right to privacy,
right to data protection,
fundamental human rights,
medical data protection

https://doi.org/10.18690/mls.17.1.89-108.2024
CC-BY, text © Turnšek, 2024
This work is licensed under the Creative Commons Attribution 4.0 International License.
This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use.
https://creativecommons.org/licenses/by/4.0

University of Maribor Press

1 Intrudaction

Data protection is increasingly becoming a topical field of study. Primarily, it is not recognized as a fundamental human right, but instead only as an obligatory part of almost every administrative procedure. Especially following the Covid-19 crisis onwards, a large amount of confidential personal data regarding people's health circulates among healthcare providers. Accordingly, it is reasonable that the security requirements necessary to securely process, collect, store, transmit and use data vary and are now rapidly evolving.

The article first examines the historical underpinnings of the right to data protection, starting with the work of founders of the medical world and progressing to the adoption of the General Data protection Regulation[1] (hereinafter: GDPR). The article then analyses three related rights – the right to human dignity, the right to privacy and the right to data protection – and compares them in view of both legislation and legal theories. Thirdly, the article assesses the relevant case law of The European Court of Human rights (hereinafter: ECtHR), by exposing some serious violations related to the right to (medical) data protection of individuals and establishes the aim of ECtHR's data protection pursuant to Article 8 ECHR.

The article may serve us as a tool to recognize similar cases that are yet to arise at the national level and rather stimulate those to be solved before the national courts, instead of taking individuals to a decade long pleading before the ECtHR. In a superior potential, the article shall suggest where the most critical loopholes lay and prevent such situation (or violations) from occurring in the first place. The following work is based on empirical legal studies and refers to many topical cases of the ECtHR.

2 Historical overview

While data protection is still a topical subject matter, it has ancient historical roots. The importance of protecting personal data was recognised centuries before Christ, in the times of Hippocrates, the father of modern medicine. Its awareness continued

[1] 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) (Text with EEA relevance), OJ. L 119, 4.5.2016.

through the work of Florence Nightingale, who is better known as "*the lady with the lamp*" or the founder of modern nursing and through activities of other pioneers in the field of medicine. The Hippocratic Oath can be interpreted as *a commitment to excellence* in the life and medical practice of the physician (Močnik Drnovšek, 2008, pp. 33-51). In order to reach its high professional and moral standards, the Oath sets out three principles: respect for the sacredness of life, protection of privacy and acting in the best interests of the patient (Loeffler, 2002, p. 1463). Furthermore, chapter seven of the Oath particularly provides that doctors are bound to keep confidential all information disclosed to them concerning the lives of patients and their families. In doing so, the doctor commits to respect the confidentiality of this information and the privacy of the individual (Močnik Drnovšek, 2008, pp. 33-51). While in around 400 BC this was called a mere oath, today it is called the protection of the right to privacy, personal data and dignity, or more generally, the protection of human rights.

Through the past decades, human rights and fundamental freedoms have become increasingly important as evidenced by their inclusion in the highest legal acts of all democratic states (e.g. in Slovenia, human rights are founded in its constitution, Ustava Republike Slovenije[2]). The Magna Carta Libertatum, in the year 1215, was the first legal act to formally grant the right to privacy for individuals. In 1776, the United States of America recognized the protection of human rights as we know it today in the Declaration of Human Rights. While these were remarkable achievements in their times, the respect of rights and declarations collapsed in the 19th century as a consequence of the First and Second World Wars. As a response to massive violations of human rights during the Wars, and also in light of the Universal Declaration of Human Rights of the United Nations, the Convention – now known as the European Convention on Human Rights (hereinafter: ECHR)[3] was accepted. All of the EU Member States (hereinafter: MS) and other signatories had adopted the ECHR and embraced its provisions as a fundamental part of each state's domestic legal system. As signatories to the ECHR, they recognized the primacy of human dignity as an absolute right.

[2] Ustava Republike Slovenije (Constitution of the Republic of Slovenia - CRS): Uradni list RS, no. 33I/91, 42/97, 66/00, 24/03, 69/04, 69/04, 69/04, 68/06, 47/13, 75/16, 92/21.
[3] European Convention for the Protection of Human Rights and Fundamental Freedoms of Council of Europe, as amended by Protocols Nos. 11 and 14, ETS 5, 4 November 1950.

Unfortunately, as often is the case with the fast-paced development of the healthcare sector, more particularly of the technological-information systems such as eHealth and eReceipt, evolution of regulations and law barely lagged behind. It is a notorious fact that law always follows the society and its changes, thus regulations usually change only when problems occur. Quite recently, MS have had to adapt their legal acts regarding data protection because GDPR has changed the narrative of the data protection as it was set out before with the Directive 95/46/ES.[4] In particular, it has generated new demands and regulated the field of studies more precisely. In parallel, the European Commission announced its eHealth Action Plan and demonstrated how all MS shall modernize the structures of their health systems and upgrade them with various e-tools. Although the Plan was designed in 2004, some MS needed more than 15 years to "fulfil" it. For example, Slovenia's government started executing the plan in 2015 and failed to complete it until the epidemic (Rant, 2018, pp. 180-183). The outburst of Covid-19 emphasized the need for such technological improvements and contributed to the Plan being implemented faster. However, the legal acts governing the relevant field are adapting slowly and new legal acts are still in in the development phase. Some MS have already developed a well-functioning framework (e.g. Finland), some are still in the process of transition (e.g. Slovenia) while others lag even further behind (e.g. Portugal) as the Slovenian Ministry of Health assessed in the draft of Health-Information System Act.[5] Considering the *new* structure of Slovenian information-technology system in health sector, the regulations have been exercised and some changes had already been made, such as the more detailed regulation of the system eZdravje, improving its transparency, administration and control over this application as well as the security of such enormous mass of private personal-health data. It is important to recognize that any loopholes in legislation may result in breaches in the health sector including in the sense of violations of human rights or exploitation of the system.

[4] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.
[5] Ministry of Health RS, Predlog zakona o zdravstvenem informacijskem sistemu (*Draft of Health-Information System Act*). Retrieved from file:///C:/Users/1262/Downloads/o_VG_JR_04042023.pdf (November 20, 2023).

3 The right to human dignity, privacy and data protection through theory and legislation

This article draws an overview of the individual's right to data protection, particularly in the sphere of health services. By protecting patient's data, it is not only data that is protected, rather patient's privacy and their dignity. Therefore, the following chapter will explain what each of the following means and expose some parallels and distinctions between them.

3.1 The right to dignity

In his book 'Human Dignity', George Kateb, who is an influential political theorist and a professor at Princeton University, advances the broad proposition that dignity is essential to the idea of human rights, and further suggests that human rights actually derive from human dignity, which represents a central part of the human condition (Kateb, 2014, pp. 1-27). The right to human dignity has more than one purpose and thus may be understood as a right, as a value or even as both-combined (Rinnie, 2016, p. 4). As a right, it is constituted directly in Article 1 of the Charter of Fundamental Rights of the European Union (hereinafter: the Charter)[6], which states that the individual's dignity is inviolable and has to be respected and protected. However, in the ECHR the following right is implied indirectly, meaning it is included in the rights, such as prohibition of torture (Article 3 ECHR), prohibition of slavery (Article 4 ECHR), the right to private and family life (Article 8 ECHR), in the prohibition of discrimination (Article 14 ECHR) and more.

Admittedly, its meaning is very broad, numerous definitions try to articulate it but any precise one turns elusive. Still, there are a few common qualities those different definitions share. Firstly, the right to human dignity entitles people to have equal human dignity that can neither be ignored nor diminished. Secondly, it gives people a legal basis and claim so it can (and must) be widely respected. Thirdly, it demonstrates an obligation to states, which are bound to realise the concept, right and a value of human dignity (Rinnie, 2016, pp. 4-11). In addition, the concept of dignity is a prominent source of political debates as well as of legal arguments (McCrudden, 2013, p. 500). For instance, the ECtHR implied that the recognition

[6] Charter of Fundamental Rights of the European Union, OJ EU C 326, October 26, 2012.

of dignity means both the recognition of the value of the individual and recognition of one's right to autonomous decision-making (see case *I. v. Finland* (2008) app. no. 20511/03). However, its meaning varies among jurisdictions and within a particular jurisdiction throughout time (McCrudden, 2008, pp. 655-724). In Opinion 4/2015,[7] The European Data Protection Supervisor expressed concerns regarding the digital processing, collection and transmission of data in a way that the person whom the data concerns must remain considered as an individual and not simply as a consumer or user in order not to diminish the subject's dignity.

To summarize, the right to human dignity is more of a concept than of a right, yet it is of fundamental value for human rights in general. It represents a foundation of the right to privacy and consequently, of data protection.

3.2 The right to privacy

The right to privacy is a right deriving directly from the right to human dignity. The right to privacy was created in the following years after World War II and in consideration of the latter, state constitutions initially protected only those aspects of privacy that were breached at the time – the sacredness of home and of correspondence (Diggelmann & Cleis, 2014, pp. 441–458). The health sector did not fall in that loop and consequently, it did not benefit from these reforms. Patients' rights had not yet been acknowledged and thus, the right's potential and scope was overlooked or maybe even underestimated.

Today, the right to privacy stands for one of the personal rights, of which aim is to directly and exclusively protect the human personality and one's physical and moral spheres (Krušič Mate, 2010, pp. 11-17). It is an absolute right, meaning no one can interfere with it.[8] The right to privacy protects the sanctity of one's personal and family life, including everything subsumed within this sphere together with all personal information, which an individual wants to keep inviolate (Krušič Mate, 2010, p. 16).

[7] European Data Protection Supervisor, Opinion 4/2015 Towards a new digital ethics - Data, dignity and technology. Retrieved from 15-09-11_data_ethics_en.pdf (europa.eu) (November 16, 2023).
[8] However, it is still bound by the boundaries of other rights and it cannot be understood as narrow as one of substantive rights, e.g. property right.

The right is enshrined in domestic as well as in many international legal acts (ECHR, The Declaration of Human Rights, the Charter, GDPR, etc.). Article 8 of the ECHR includes it in the right to respect for private and family life. So does the Charter in Article 7. The Charter states that the right comprises the right to respect for private and family life, as well as respect to home and communications. In comparison to the Charter, the ECHR is written more precisely as it adds the additional paragraph. The second paragraph contains language that explicitly prohibits any interference into a person's private life by a public authority (except if there is a legal basis or legitimate aim, such as public interest). Importantly, there are two different aspects of privacy protection. The individual's privacy is protected against both state's interference and from interference by another individual. Neither the state nor the third-party individual can interfere into the sphere of individual's personal life without a legal basis. The protection of privacy is critically important because the rights of privacy and to data protection enable individuals to develop their own personalities, to have their own independent lives and to practise other rights or freedoms (as explained in the already mentioned Opinion 4/2015). Considering health services, out of respect for the privacy of a patient, the ECtHR confirmed domestic laws must guarantee safeguards to prevent any unnecessary disclosure of personal health data (see cases: *I. v. Finland* (2008) app. no. 20511/03, *Z v. Finland* (1997) app. no. 22009/93, *Y.G. v. Russia* (2022) app. no. 8647/12, *Avilkina and others v. Russia* (2013) app. no. 1585/09 etc.). Those decisions have precedential value and apply to all states signatories.

In general, a patient's right to privacy and confidentiality is one of the fourteen rights they enjoy. Article 35 of the Charter elaborates that medical services at the national level will be assured at a high-quality level with an aim to generally guarantee a great level of health protection in all MS. Therefore, it can be assumed that when having any kind of medical treatment, the fourteen patients' rights are one of the first points to be fulfilled. Pursuant to Slovenian legislation, its constitution Ustava RS[9] in Article 35 broadly states that an individual's privacy and personal rights are guaranteed. These rights are further on substantiated in various secondary legal acts, and are realised and practiced during common healthcare procedures and routines, such as office visits, laboratory testing etc.

[9] Ustava Republike Slovenije (Constitution of the Republic of Slovenia - CRS): Uradni list RS, no. 33I/91, 42/97, 66/00, 24/03, 69/04, 69/04, 69/04, 68/06, 47/13, 75/16, 92/21.

Therefore, all patients' rights, including the right to privacy and confidentiality, are protected throughout the entire EU. All information relative to an individual's state of health, and to their treatments, should be considered as private, and per se, sufficiently protected. Pursuant to the European Charter of Patients' rights,[10] various treatments, such as diagnostic exams, visits of specialists, etc., must occur in *an appropriate* environment and only in the presence of persons whose presence is necessary. Even so, in practise some serious breaches still occur, as evidenced by a 2015 Slovenian Supreme Court case[11], where a doctor allowed his 13-year-old son to assist him during two surgeries. Even though the other staff opposed the son's involvement, the doctor ignored them, allowing the son not only to observe, but to actively engage doing stiches and similar activities. The doctor's actions violated many of the patient's rights, especially the right to privacy and confidentiality, the right to the observance of quality standards, the right to safety and more. Ironically, the case did not reach the Supreme Court in the context of the patients claim for breach of patient's rights, but instead arose in the field of labour law.

Finally, the right to privacy is certainly more concrete than a conceptual right to human dignity considering all the substantive law and regulations. Even though it may be understood as if the right to privacy was based on the right to human dignity (see Floridi, 2016, pp. 307-312), or as if it was a part of it, privacy protection lies within its own sphere and guards more specific areas of human physical and moral attributes.

3.3 The right to data protection

The right to data protection is narrower in comparison to the right to privacy and presently, it is the subject of intense scrutiny. If we consider the right to dignity as "a trunk of a tree" and the right to privacy as a "thicker branch" on the tree, then by further analogy the right to data protection should be understood as a "leaner branch" stemming from the broader right to privacy.

[10] Active Citizenship Network, European Charter of Patients' rights Basis document. Retrieved from Microsoft Word - Final Draft.doc (europa.eu) (November 16, 2023).
[11] Sodba Vrhovnega sodišča RS (*Judgement of the Supreme Court of the Republic of Slovenia*) of 27 October 2015, VIII Ips 114/2015, ECLI:SI:VSRS:2015:VIII.IPS.114.2015.

The right to data protection is subsumed in the scope of the right to privacy and as well as the latter, it suggests its absoluteness against everyone, including the state (Krušič Mate, 2010, p. 12). The right to data protection is, similarly to the right to privacy, protected directly or indirectly by the highest domestic, EU and international acts (ECHR, The EU Charter, GDPR, constitutions of democratic states etc.) One of the primary legal acts of the EU – the EU Charter (as well as the GDPR) proposes data protection principles, which are necessity, proportionality and fairness, data minimisation, purpose limitation, consent and transparency. Pursuant to Opinion 4/2015, those principles apply to data processing, collection and to its use to secure individuals' privacy. Considering that a large amount of confidential personal health data of a very sensitive nature circulates among healthcare providers, it is important that this is done with respect to the foregoing principles. Furthermore, unlike the other international human rights' legal acts, Article 8 of the EU Charter sets out a right to data protection as a completely independent right – not as a subcomponent of the right to privacy like interpreted in the ECHR (Lynskey, 2014, pp. 569-597). The Charter establishes the protection of individual's data and notes that the suggested provisions must be under control of an independent authority.[12] Paragraph two of Article 8 of the Charter even provides that data should be processed fairly, with a definite purpose(s), on the grounds of concerned individual's consent (or on other legitimate or legal basis). It specifically states that every individual has the right to access the collected data regarding them and to demand necessary corrections.

Furthermore, the EU confirmed its importance in many secondary legal acts, among which the latest regulation – the GDPR, serves as "the Bible" to all MS in the field of data protection. Thus, the inclusion of the right to data protection in human rights legal acts signifies its overarching importance, and confirms that the GDRP constitutes the general legal basis for the content of data protection law in MS' legal systems. While the GDRP applies directly to all MS, the MS had (and still have to) to change their domestic regulations to comply with the EU rules in order to realise the harmonization of the EU legal order. Admittedly, GDPR allows MS to regulate particular areas of data protection completely on their own (e.g. Article 9 GDPR proposes that regarding genetics, biometric and other health issues, the MS can propose other or extra requirements). Moreover, in connection to particular articles

[12] See the 1st and the 3rd provision of the Article 8 of the Charter.

and provisions of GDPR, the States are also given "the freedom of its usage" to some extent. This means that in some cases the MS can choose between the use of various points the provision sets out. For instance, Article 6 of the GDPR states that processing of data is considered lawful only if at least one of the required conditions (given consent, performance of a contract, compliance with a legal obligation, protection of the vital interests, public interest and legitimate interest) applies. Therefore, a particular MS can choose any of the listed requirements and use it according to what will be well-accepted and what will function well in its legal system, while simultaneously being in sync with the provisions of GDPR. Interestingly, according to the document Assessment of the EU Member States' rules on health data in the light of GDPR[13], the "protection of vital interests" requirement is used the least. What is more, for every specific area, there is another specialized domestic legal act, which lays down the provisions, specific to its field of studies and accordingly demonstrates, which rules from the GDPR are applicable. For instance, pursuant to Slovenian healthcare system in connection to data protection of a patient, the most relevant legal act is the "Patient Rights Act"[14], followed by "Databases in Healthcare Act"[15], "Health Services Act"[16] and others. Specifically, Chapter 13 of the Patient Rights Act[17] sets forth provisions regarding the patient's right to privacy and data protection, relevant while providing health services (e.g. Article 43 PRA – "privacy when providing a health service", Article 45 PRA – "protection of professional secrecy"). Since data protection reaches all fields of studies and work, it would be rather impossible to predict all the specifics in one general act.

Undisputedly, the ECHR is another important human rights act resting outside of the EU regulatory framework. Article 8 ECHR includes the narrower protection of personal data within the broader right to respect for private and family life. Pursuant to Article 8 ECHR, everyone shall be provided with the right to a home, to correspondence and to respect for his or her private and family life, and at the same

[13] European Commission, Consumers, Health, Agriculture and Food Executive Agency, Hansen, J., Wilson, P., Verhoeven, E. et al., Assessment of the EU Member States' rules on health data in the light of GDPR. Retrieved from https://data.europa.eu/doi/10.2818/546193 (November 5, 2023).
[14] Zakon o pacientovih pravicah (*Patient Rights Act – PRA*): Uradni list RS, no. 15/08, 55/17, 177/20, 100/22.
[15] Zakon o zbirkah podatkov s področja zdravstvenega varstva (*Databases in Healthcare Act*): Uradni list RS, no. 65/00, 47/15, 31/18, 152/20, 175/20, 203/20, 112/21, 196/21, 206/21, 141/22, 18/23, 84/23.
[16] Zakon o zdravstveni dejavnosti (*Health Services Act*): Uradni list RS, no. 23/05 (OCV1), 15/08, 23/08, 58/08, 77/08, 40/12, 14/13, 88/16, 64/17, 1/19, 73/19, 82/20, 152/20, 203/20, 112/21, 196/21, 100/22, 132/22, 141/22, 14/23, 84/23.
[17] Zakon o pacientovih pravicah (*Patient Rights Act – PRA*): Uradni list RS, no. 15/08, 55/17, 177/20, 100/22.

time be protected from unlawful interference by public authorities (except in exceptional cases provided by law). Accordingly, even though the right to data protection is included in the overarching right or laws under covering name, that does not suggest the right would be any less important or any less protected. That was confirmed with many decisions of the ECtHR, which will be discussed in the following chapter.

Based on the research at hand, data protection is not a "smaller" right than the right to privacy, instead it only derives from it. Both rights are derived from the human rights act(s) and are buttressed through secondary legislation. Similarly, they protect an individual's private sphere to some extent, the right to privacy in the broadest sense and the right to data protection in a more specified way. Respecting either one may equal respecting an aspect of human dignity. For instance, a doctor that respects a patient's right to privacy by not sharing information regarding the patient's mental disorder diagnosis concomitantly protects the patient's dignity. However, the converse is not necessarily true. If, by way of example, someone respects an individual's right to human dignity by not sexually assaulting them, that has nothing to do with respect of the right to data protection. In conclusion, although the connection between the rights cannot be neglected, there are important distinctions between them, giving each its own purpose.

4 Data protection through the prism of case law

Considering the benefits of developing technologies, which ease our daily lives and save us from various tasks, it is only natural to expect they will expand and spread to all sectors and activities, including to the health sector. The EU's plans (digital single market, cloud computing, the 'Internet of Things', big data etc.) are now seen as vital to competitiveness and growth, which was confirmed through The European Data Protection Supervisor's Opinion 4/2015. In this regard, as companies, businesses and state's entities deal with massive amounts of personal data, which are processed, collected, transmitted, used and reused on a daily basis, the latter has to be justified on the grounds of law or privacy policies. Further on, the text will focus specifically on the cases of the ECtHR, in which the national legal systems in various European states failed to protect personal-medical data of patients.

In the case *Y.G. v. Russia*[18], the plaintiff diagnosed with HIV and hepatitis purchased a database on the Moscow market that included personal data from more than 400,000 individuals from Moscow or that region, each infected with HIV, AIDS or hepatitis. In this database, he found, among all other information, his personal and medical data. The plaintiff pursued legal remedies at the national level, i.e. in Russia, but without any success. As the State failed to protect the plaintiff's medical data and his right to data protection, the case was referred to the ECtHR for a violation of Article 8 ECHR, which ultimately confirmed the violation. Ensuring the right to privacy and the confidentiality of personal data is crucial, particularly concerning the protection of information relating to HIV or a comparably sensitive condition. The disclosure of such information to the public may have an extremely negative impact on an individual's private and family life, on his or her social and professional standing, and it may lead to exposure to stigmatisation and possible exclusion of that individual.[19]

Even during criminal investigations, national authorities must strike an appropriate balance between the individual's right to respect for private life and the protection of public health and public safety. A case in point is *Avilkina and others v. Russia*[20], where the criminal investigation interfered with personal data of Jehovah's Witnesses. After Jehovah's Witnesses had already refused blood transfusions, state hospitals disclosed their medical records to the prosecutor. The unlawful activity consisted of the fact that Jehovah's Witnesses were neither informed nor given the opportunity to object or to consent. The State's actions constituted a disproportionate interference with the Jehovah's Witnesses' right, resulting in a violation of Article 8 ECHR. The ECtHR has clarified that the collection of confidential medical information by judicial authorities is compatible with Article 8 ECHR and permissible, but only when accompanied by sufficient safeguards.

The ECtHR declared another breach of Article 8 ECHR in the case of *Z. v. Finland*[21]. The plaintiff (Ms. Z) was married to the defendant, who infected her with HIV. In the court proceedings, sensitive personal-health data regarding the infection and Z's

[18] Judgment of the ECtHR of 30 August 2022, 8647/12, Y.G. v. Russia.
[19] European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence. Retrieved from Guide on Article 8 - Right to respect for private and family life, home and correspondence (coe.int) (November 19, 2023).
[20] Judgment of the ECtHR of 6 June 2013, 1585/09, *Avilkina and others v. Russia.*
[21] Judgment of the ECtHR of 25 February 1997, 22009/93, *Z. v. Finland.*

mental state were shared, despite her disagreement. In the decision ECtHR, as with the preceding case, pointed out the importance of respecting the confidentiality of an individual's medical information by describing it as a significant principle in the legal orders of all the Contracting Parties to the Convention. The Court underlined this is crucial not only to respect the patient's privacy, but also to maintain their trust in the medical profession and in health services in general. The ECtHR further explained that a failure to guarantee protection of personal data could discourage persons in need of medical assistance from seeking medical services. Therefore, national legislation must provide sufficient safeguards to prevent the possibility of breaches, or non-obedience and to shield the guarantees set out in Article 8 of the ECHR.

Finland, *I. v. Finland*[22], involved the disclosure of HIV information. The plaintiff, who was a nurse employed in a public hospital's polyclinic for eye diseases, had also been visiting an infectious diseases polyclinic at the same hospital, due to her HIV infection. Based on co-worker's comments and observations, she started suspecting they had unlawfully accessed and read her medical records. By doing so, her colleagues had not only learned of her state of health, but had also committed many violations, including violations of human rights. The unwarranted access and unsubstantiated colleagues' knowledge of her medical condition resulted in violations of respect for dignity, of the right to privacy and of the right to make autonomous decisions regarding the communication of her illness to third parties. The violation of plaintiff's right to privacy resulted in the loss of her employment as her employer did not renew her contract. The Court found that the plaintiff lost her civil action in the proceedings before domestic courts, because she could not prove the connection between deficiencies in the access security rules and the spread of information about her medical state. Arguably, the Court stressed that to burden an individual with proving such a connection is tantamount to overlooking the acknowledged deficiencies. The Court, in other words, was concerned the lower Courts had imposed upon the plaintiff an impossible burden: proving the negative. The ECtHR confirmed an unlawful disclosure of personal data, resulting in insufficient protection of her right to private life pursuant to Article 8 ECHR.

[22] Judgment of the ECtHR of 17 July 2008, 20511/03, *I. v. Finland.*

P.T. v. The Republic of Moldova[23] again involved a plaintiff who is HIV positive. Plaintiff was a soldier that underwent a medical examination at a Military Centre to obtain a military service record book. He himself informed the doctors about his HIV infection, which they confirmed. The Military Centre later issued him "the exemption certificate" in place of the military service record book, according to which he was exempted from military service in line with the Medical Standards provided for by Defence Ministry. Moreover, when plaintiff learned he was getting his national identity card, which is obligatory under their national law, he had to produce his military service record book or the exemption certificate. To fulfil this obligation (which he did), he had been required to disclose his personal medical data to various authorities. At the ECtHR plaintiff claimed his right to personal protection of his health data pursuant to Article 8 ECHR was breached. Ruling in favour of the plaintiff, the court stressed that any disclosure of an individual's medical information presents a disproportionate interference with the right to protection of private and family life. The Court explained that "systematic storage and other use of information" by authorities, if connected to the right to private life, comprises an interference with the relevant rights (see the paragraph no. 26 of the case of the present case). Admittedly, the more intimate and sensitive the information processing affects (such as information relating to physical or mental health of an individual), the more important and applicable the latter is. The ECtHR concluded that the Government did not have a legitimate aim and consequently, plaintiff's privacy rights under Article 8 ECHR were violated. The Court considered the Government's interference as a serious breach of the principle of proportionality.

In *Surikov v. Ukraine*[24], plaintiff Surikov graduated from technological engineering and worked in a state-owned company. In 1997, after seven years of working there, Surikov asked the director to place him on the reserve list for promotion to an engineering position, which would be equivalent to his qualifications. Three years later, after not getting any feedback, Surikov reapplied, but his renewed application was again denied. In this regard, Surikov filed an appeal with the Central District Court. During the proceedings, the company revealed that its refusal was related to applicant's mental health gleaned from information in the applicant's personnel file.

[23] Judgment of the ECtHR of 26 May 2020, 1122/12, *P.T. v. The Republic of Moldova.*
[24] Judgment of the ECtHR of 26 January 2017, 42788/06, *Surikov v. Ukraine.*

Specifically, in 1981, he had been affirmed as unfit for military service in peacetime pursuant to the binding legislation. The company's HR department got a certificate from the military enlistment office, which asserted the applicant had been dispensed, because of the following diagnosis: "psychosis and psychotic disorders connected to organic cerebral lesions with residual moderately manifested deviations in the mental sphere". As Surikov did not provide any information regarding the state of his mental health, the company claimed his promotion to an engineering position (consistent of management-responsibilities, supervision of other employees) was regarded as *unwarranted*. The proceeding proceeded all the way to the Supreme Court, but Surikov's claim was rejected. He then underwent medical testing and obtained a certificate, signed by six medical specialists, verifying his capability to work as an engineer. Surikov started another procedure against the company, in which he claimed damages and demanded apologies for the unlawful processing of his health data and discrimination based on health. This proceeding again resulted in a ruling in favour of the company. Surikov instituted a third action, this time not against the company, but against its officers because of their unlawful actions in connection to data protection. Even though Surikov argued that the subject information "had been outdated, incomplete and impertinent" and that his employer should have checked his health status, the court refused his claims and decided in favour of the officers. Eventually, the case reached the ECtHR, which stressed that such (medical) information represents highly sensitive personal data. Therefore, any collection, storage, disclosure and other types of processing of such information fall within the scope of Article 8 ECHR. Additionally, the interference in Surikov's right to private life was made by a public authority (since the company was state-owned). The Court explained that the basic principles of data protection demand proportionality in relation to the purpose of collection. In this regard, the employer's retention of sensitive medical data pertaining to their employees is lawful under Article 8 ECHR only if there are strong procedural safeguards in place, ensuring "such data would be kept strictly confidential, would not be used for any other purpose except for which it was collected, and would be kept up-to-date". In the present case, the Court considered the company's interference as disproportionate and unnecessary. Unsurprisingly, the Court finalized its decision by declaring that the disclosure of Surikov's health data violated Article 8 ECHR. In 2006, Surikov became an engineer-technologist.

The ECtHR arrived at an even more far-reaching conclusion in the case *Y.Y. v. Turkey*[25], where the main question was when do trans-genders have a right to legally change their gender. Turkey's national regulations had set out an obligatory medical requirement, which prescribed that an individual has to medically change their gender (go through surgery of sterilization) so he or she is then able to change it legally. The Court reasoned that gender recognition comprises a very intimate side of an individual's identity, meaning it is "one of the most basic essentials of self-determination" (see paragraph 102 of the present case). As the Court recognised many states have the same requirement, (so most likely those states would neither pass the test under Article 8 ECHR), it also stressed that the circumstances, combined with international and European law and practise have to be taken into account. Hence, it emphasized the case at hand had to be assessed "in the light of present-day conditions". Finally, the Court reasoned that the regulation of gender reassignment surgery is not a necessary condition, thus it cannot be regarded as sufficient. The ECtHR confirmed the State breached plaintiff's right to respect for his private life and consequently violated Article 8 ECHR. Admittedly, this case was not of particular importance for the field of data protection, rather for the development of the right to privacy and for trans-gender community in general. Nevertheless, the Court's decision presents an important and far-reaching finding that should affect all other States having legislation including the same requirement as that in Turkey.

Taken together, the results of these cases lead us to the final conclusion, namely that the right to personal data is quite often insufficiently regulated or ineffectively protected at the national level, meaning by domestic courts and/or legislation of the States Parties to the ECHR, as serious violations of the Article 8 ECHR continually occur. The ones who have both the power and the obligation to prohibit such violations are the States. Notably, even though the safeguards have to be proposed by a particular state or its public authorities, that caveat does not exclude them from prohibiting any interference with an individual's right. Stated differently, as is the case with private individuals, the public authorities too must abide with the safeguards that prevent them from interfering with an individual's right to respect for private and family life. The case law also is instructive on the importance of keeping sensitive medical data sacred and safe. By doing so, individual's privacy and

[25] Judgment of the ECtHR of 10 March 2015, 14793/08, *Y.Y. v. Turkey*.

dignity shall stay protected. If not, individual's privacy and dignity shall become desecrated, which may result in social stigmatisation or exclusion as well as the loss of that person's trust in health services. The latter could lead to the situation where the person impacted fails to seek medical services, which could endanger not only their own lives or (if the disease was highly transmittable) but even society as a whole.

5 Conclusion

The rights to human dignity, privacy and to data protection, though separate in theory, are interconnected rights. In comparison to the right to human dignity, which protects an individual from the broadest scope of violations, the right to data protection safeguards the most limited number of breaches. The mentioned rights have foundation in the highest international legal acts, such as ECHR, The Charter and Declaration of Human Rights, while they are also included and substantiated in the domestic legislation and various secondary legal acts. In addition, besides the raw legislation, there are also courts, confronting concrete cases and trying to regulate a correct application and sufficient respect of the right to data protection.

The ECtHR in particular has established an extensive base of cases, confirming the importance of the right pursuant to its Article 8, mainly for the following reasons. The Court's aim is to prevent individual's stigmatisation or social exclusion, as well as to protect their mental and physical well-being and in general, their integrity. Through its judgments, the ECtHR established the sacredness of an intimate side of individual's identity. It has done so by being very strict on what does and does not constitute a necessary and sufficient interference into an individual's privacy (see cases: *Y.Y. v. Turkey* (2015) app.no. 14793/08, *Surikov v. Ukraine* (2017), app. no. 42788/06, *Y.G. v. Russia* (2022) app. no. 8647/12). Importantly, the interference by a public authority of any kind has a very "limited frame of allowed interference", which has to be justified by law and in concrete situations determined as necessary and sufficient.

Hence, the protection must be even greater when it comes to cases involving medical data, which are per se sensitive and intimate. Consequently, its revelation might have an immense influence on the individual's life. In another aspect, by protecting an individual's medical data, people will feel safe in the medical institutions and will not stop seeking medical services out of fear that their sensitive medical data could at

any point be revealed. Otherwise, people could lose their trust in health services and stop seeking them. This could have disastrous consequences such as the collapse of health services and people not securing medical treatment for various diseases, which not only endangers themselves, but also the greater society. Such activity would be in contradiction to the broader principle of public good and public interest. Most importantly, both possible outcomes would be negative and damaging for the society as a whole as well as for individuals and their health.

Finally, the objective of the right to data protection as a human right is in general to secure individual's private sphere and human integrity. There are many cases – older ones as well as new ones, proving the individual does not have a sufficient protection before the national courts. Admittedly, the field of data protection and the field of technological-information systems in healthcare are each in their fast-paced development era and it certainly is a challenge to follow up and put such complex theory into practise. However, that is court's task and should not be neglected, not at the first instance and even less likely at the higher or Supreme Court of any democratic country.

References

Diggelmann, O., Cleis, M. N. (2014). How the Right to Privacy Became a Human Right Get access Arrow. *Human Rights Law Review,* 14(3), 441–458.

Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. *Philosophy & Technology*, 29, 307–312.

Kateb, G. (2014). *Human Dignity*. Cambridge: Harvard University Press.

Krušič Mate, Z. (2010). *Pravica do zasebnosti v medicini*. Ljubljana: GV Založba.

Loeffler, I. (2002). Why the Hippocratic Ideals Are Dead. *The BMJ*, doi: https://doi.org/10.1136/bmj.324.7351.1463.

Lynskey, O. (2014). Deconstructing data protection: The 'added-value' of a right to data protection in the EU legal order. *International & Comparative Law Quarterly,* 63(3), 569-597.

Močnik Drnovšek, V. (2008). Hipokratova prisega in njen pomen za medicinsko deontologijo. *Keria*, 1, 33-51.

McCrudden, C. (2008). Human Dignity and Judicial Interpretation of Human Rights. *European Journal of International Law,* 19(4), 655–724.

McCrudden, C. (2013). *Understanding Human Dignity (Research Output)*. Oxford: Oxford University Press.

Rant, Ž. (2018). Projekt eZdravje v Sloveniji - vsebinski in zgodovinski pregled. *30 let Slovenskega društva za medicinsko informatiko*, 180-183.

Rinnie, S. (2016). The core meaning of human dignity. *African Journals Online,* 19, 4- 11.

Povzetek v slovenskem jeziku

Ali so osebni podatki in informacije, ki jih v celoti zaupamo zdravstvenim sistemom, dovolj zaščiteni? Članek obravnava križišče prava in medicine, in sicer v točki, kjer je pravica do varstva podatkov pacienta kršena ali zakonsko nezadostno zaščitena. V zvezi s tem moramo najprej spoznati, kakšen je dejanski obseg pravice posameznika do (medicinskega) varstva podatkov in drugič, razumeti, kdaj je ta pravica kršena. Članek analizira izvor varstva podatkov in njegov zgodovinski razvoj, z namenom najti njegov osrednji pomen. Nadalje išče meje obsega varstva podatkov z vsebino drugih sorodnih pravic. S celovitim pregledom evropske sodne prakse članek razkriva nekatere resne kršitve pravice posameznikov do (medicinskega) varstva podatkov.