Nanoethics (2022) 16:297–312
https://doi.org/10.1007/s11569-022-00431-0

ORIGINAL RESEARCH PAPER

Reflections on Turkish Personal Data Protection Law and Genetic Data in Focus Group Discussions

Özlem Özkan · Melike Şahinol · Arsev Umur Aydinoglu · Yesim Aydin Son

Received: 6 July 2022 / Accepted: 18 November 2022 / Published online: 7 December 2022

Abstract Since the 1970s and more rigorously since the 1990s, many countries have regulated data protection and privacy laws in order to ensure the safety and privacy of personal data. First, a comparison is made of different acts regarding genetic information that are in force in the EU, the USA, and China. In Turkey, changes were adopted only recently following intense debates. This study aims to explore the experts' opinions on the regulations of the health information systems, data security, privacy, and confidentiality in Turkey, with a particular focus on genetic data, which is more sensitive than other health data as it is a permanent identifier that is inherited to next of kin and shared with other family members. Two focus groups with 18 experts and stakeholders were conducted, discussing topics such as central data collection, legalized data sharing, and the management of genetic information in health information systems. The article concludes that the new Turkish personal data protection law is problematic as the frame of collectible data is wide-ranging, and the exceptions are extensive. Specific laws or articles dedicated to genetic data that also overlook the dimension of discrimination based on genetic differences in Turkey should be taken into consideration. In broader terms, it is intended to put up for discussion that in addition to ethical aspects, economic aspects and legal aspects of health should be included in the discussion to be carried out within the framework of socio-political analyses with culture-specific approaches and cross-culture boundaries simultaneously.

Keywords Data protection · Data privacy · Genetic data · Turkish personal data protection law · Focus group

Background

The first significant step to framing standards for the protection of individuals was taken with the Universal Declaration of Human Rights after the Second World War. It was adopted by the General Assembly of the United Nations (UN) among the UN member countries on December 10th, 1948. Even though it has been translated into 370 different languages and

Ö. Özkan
Berlin, Germany
e-mail: ozlemkan@gmail.com

M. Şahinol (✉)
Orient-Institut Istanbul, "Human, Medicine and Society",
Istanbul, Turkey
e-mail: sahinol@oiist.org

A. U. Aydinoglu
Science and Technology Policy Center, Middle East
Technical University, Ankara, Turkey

Y. Aydin Son
Department of Health Informatics, Middle East Technical
University, Ankara, Turkey

became the most translated document in the world [1], it was not a legally binding declaration. Five years later, the European Convention on Human Rights was entered into force (September 3rd, 1953), and the Council of Europe member countries ratified these rights in order to become binding for the member states. They, then, adapted their national laws to give effect to the European Convention on Human Rights [2]. Unlike them, the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data ("Convention 108"), which the Council of Europe adopted in 1981, obliged signatory countries to apply the principles of processing personal information. Moreover, this time, the Convention was also open for signature to countries outside Europe. Although Turkey became one of the countries which signed the Convention on the same date it was released, the first draft of the current Personal Data Protection (PDP) law was prepared several years later (2003) [3].

As time progressed and new technologies evolved, systems and methods for collecting and processing data varied and became extremely complicated. As a result, many countries (mainly in Europe) started to update their legislation and added specific rules about how privacy should be managed [2]. This growing diversity in national data protection approaches was interpreted as an obstacle to the completion of the internal market by the European Commission [4]. The commission commented: "If the fundamental rights of data subjects, particularly their right to privacy, are not safeguarded at the community level, the cross-border flow of data might be impeded" [4]. Thus, in 1995, the Data Protection Directive was created by the European Commission and came into force in 1998 [5]. The Directive regulated that the transfer of personal information to countries outside the EU can be permitted only when the country guarantees adequate protection for the information (Directive 95/46/EC, Article 56) [5]. The Directive regulated privacy protection, and the transfer to a third country of personal data shall be provided by the member states to enforce other countries who conduct business within Europe [6, 7].

The current EU data protection and privacy regulation, General Data Protection Regulation (GDPR), was adopted on April 14th, 2016, and replaced with Directive 95/46/EC on May 25th, 2018. Only 1 week before the adoption of the GDPR (April 7th, 2016), the very first Turkish Personal Data Protection (PDP) entered into force [8]. The Turkish PDP law was prepared based on Directive 95/46/EC. However, in the EU 2018 Turkey report, the EU Commission criticized the Turkish PDP law as "the law is not yet in line with European standards" [9].

As of 2021, 145 countries, including Turkey, enacted data privacy laws [10]. Among these, European countries' regulations of the use of personal data are perceived as rather "aggressive" [11], whereas others tend to be more lenient as they give way to companies and associations regulating themselves, such as in the USA for instance, although the country later had to tighten aspects of its regulations [11]. In this paper, we discuss the Turkish PDP law within the scope of European and US regulations, a patchwork of state and national laws. Also, we will briefly mention the Chinese Personal Information Protection Law (PIPL) as these three regulations provide a suitable context in which to discuss the situation in Turkey.

The EU's current regulation GDPR is twofold; on the one hand, it provides rights and controls to data subjects, and on the other, it restricts data processors in order to mitigate risks to the rights and freedoms of people that may be caused by the processing of personal data (GDPR Article 4(7)). Health data is considered a particular category of data and, therefore, has stricter privacy regulations, so much that processing it is prohibited—except if explicit consent to processing personal data is given and used for medical purposes (GDPR Article 9(3)). This includes the health applications and wearables that collect health data.

GDPR is much more sensitive when it comes to personal data compared to the USA and China, and it provides more protection. While it defines special categories of personal data, genetic data and biometric data are singled out along with other data types, such as racial origin, trade union membership, sex life, etc., in Article 4 (13). Genetic data is identified as "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question." In Recital 34, it is defined as obtaining genetic characteristics through chromosomal, DNA, or RNA analysis (or obtaining equivalent information via another element).

Genetic analysis data may be thought of as personal data, which is fact in most cases as genetic analysis includes enough genetic markers even if names and identifiers are removed. However, anonymized or aggregated genetic sequences that cannot be linked to a specific genetic identifier are not considered personal data.

The USA offers different levels of protection for different classes of data. Each data class has different properties, such as health data, which has commercial value besides medical use. Third parties' access to health data under emergency conditions could have life-saving implications as witnessed during the COVID pandemic [12]. The variety of collected health data has increased dramatically, including clinical, administrative, genetic, behavioral, and environmental data. Simultaneously, the ability to acquire, standardize, and integrate the increasing amount of big data—and the capacity to analyze it—is expanding continuously. Applying big data analytics and AI techniques can help identify ineffective treatments, increase treatment quality, help develop new hypotheses and treatments, reduce inefficient use of resources and medical error, and monitor drug and device safety [13–15]. Moreover, it also means higher profits [16–18].

In the USA, health researchers must comply with the research-related privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA), passed in 1996, to have national standards for safeguarding the confidentiality of medical records [19]. Protected/Personal Health Information (PHI) is defined as "relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual that is transmitted by electronic media; maintained in electronic media, or transmitted or maintained in any other form or medium" [20]. So, PHI includes all information that could be used to identify an individual. Confidentiality and privacy are essential, especially with highly sensitive health data.

There are conceptual similarities between HIPAA and GDPR. However, being compliant with one of them does not guarantee compliance with the other. The USA can apply HIPAA rules while processing the data solely in the USA [21]. Nevertheless, any processing activity on the data of people in the EU must be carried out according to GDPR [21]. Two of the most significant differences are related to informed consent forms. Formerly, while GDPR's consent requirements are rigorous, HIPAA allows disclosing information without patient authorization via the approval of the institutional review board (IRB) or a privacy board [21]. Later, GDPR gives more rights—access, edit and erase—to the data subjects on their informed consent forms than HIPAA [21]. That is why HIPAA compliance may not be enough for the GDPR.

Genetic information is particularly important among other sensitive data, as it is more intimate than any other personal information [22, 23] due to its specific features, such as uniqueness, predictive capability, and impact on other family members [23–25]. Although genome sequencing and genetic tests brought incredible developments in healthcare, there are growing privacy, security, and ethical concerns regarding genetic discrimination, discrimination based on data-driven predictions of potential diseases, and genetic insurance discrimination [26–30]. The USA's Genetic Information Nondiscrimination Act (GINA) aims explicitly to eliminate these concerns. Discrimination based on genetic information in health insurance and employment is prohibited by this law in the USA [31]. President George W. Bush signed GINA in 2008, and its primary goal is to ensure the public benefit, avoid discrimination due to genetic differences by insurance companies and protect employees and applicants from discrimination [31]. On October 26th, 2016, Europe adopted a similar action, CM/Rec(201,608), regarding "the processing of personal health-related data for insurance purposes, including data resulting from genetic tests," yet another measure to safeguard sensitive data, such as genetic data, to be used by third parties for discriminatory purposes [32]. Even though there are such legal regulations, for example, in the EU Charter of Fundamental Rights, Article 21.1, there are particular areas, such as adoption agencies, fertility services, or the military, where genetic discrimination is experienced but not covered by the legislation. Hence, the debate is ongoing [33].

The protective regulations were insufficient as they were designed from the perspective of personal use; however, the accessibility to large amounts of data through two workarounds made the regulations obsolete [34]. The first one is utilizing "health-related" data, such as web searches, fitness trackers, mobile health apps, and consumer genetic services, instead of "healthcare" care data that is protected [35–37]. The second one is data extraction from HIPAA and other healthcare data regimes, which is possible since data is not regulated by HIPAA itself or whoever holds it, but by insurance-covered entities and their business associates [38]. These datasets are called shadow health records: "less-regulated records about individuals with the same sort of information as standard health records—sometimes the exact information—supplemented with data from other sources" [39]. GINA can be considered a patchwork to address this workaround [39], but better and more protective regulations came into effect through the GDPR and California Consumer Privacy Act (CCPA) of 2020. Although the GDPR is more comprehensive, the reach of GDPR outside the EU is debatable. Their fines are substantial [40]. Examples may be considered scary, such as 746 million Euros for Amazon, 226 million Euros for WhatsApp, and 90 million Euros for Google Ireland [41]. CCPA has even a smaller reach as it only applies to California residents; nonetheless, it is the most populous state with an even more significant economic influence [39]. CCPA dictates access notices and requirements for larger businesses and data brokers [42]. In short, even though there is a risk of hurting the innovative capacity among health and life sciences companies, they provide a protective capacity that has been missing [39]. That being said, it has been recommended to "bring DTC (direct-to-consumer) and PGT (personal genomic testing) companies under the umbrella of HIPAA regulations" and make GINA follow a similar suit [43].

Regarding policy on genetic data, the literature suggests three groups; regions featuring extensive policy-making activities (the USA, European Union, Canada, Mexico), regions with moderate policy-making activities (Australia, Asia, South America), and regions with minimal policy-making activities (the Middle East and Africa) [44]. However, this literature needs to be updated as China, that was not included in the analysis, introduced the Personal Information Protection Law (PIPL) in 2021 [45]. PIPL is vital because it is the only law that covers around 20% of the world's population. Moreover, it impacts multinational companies to the extent that they process the data of individuals in China. According to PIPL, medical health information is considered "sensitive personal information" along with other examples such as biometrics, religion, financial accounts, etc. [46]. Also, according to Article 33, illegally obtaining, selling, or supplying third parties more than 500 pieces of information can result in up to 3 years of detention [45]. PIPL is "both sufficiently in the mainstream of GDPR-influenced laws and sufficiently distinctive" [47] and requires more attention from scholars, for there are areas that need to be interpreted.

In conclusion, the GDPR is the most comprehensive in many areas. The US system is a patchwork of state and national laws and regulations; it is difficult to track; however, GINA, a specific genetic nondiscrimination act, serves well. The PIPL is relatively new and does not refer to genetic data specifically, instead, it has limited oversight (Table 1).

Found to be below acceptable standards by the EU report, many innovations need to be discussed in the Turkish new law, and handling genetic data is one of them. So far, there has not been any regulation dedicated to genetic data in Turkey; however, in the law, genetic data is listed in the special categories of personal data for the first time. Genetic data is listed separately from health data as well (Article 6, Paragraph 1) [8]. Therefore, the requirement for different treatment of genetic data was specified and guaranteed by law.

Hence, the study aims to explore the experts' opinions on the regulations of the health information systems, data security, privacy, and confidentiality in Turkey. This covers the current situation of the health information systems, data security, privacy, and confidentiality in Turkey, with a particular focus on genetic data, which is more sensitive than other health data as it is a permanent identifier that is inherited to the next of kin and shared with other family members.

Methodology

Focus Group Approach

We conducted *two focus group meetings* to explore the experts' opinions on the regulations of the health information systems, data security, privacy, and confidentiality in Turkey, with a particular focus on genetic data. The advantage of using focus groups as a method for evaluation is that they "provide researchers with means for collecting data that can be used to construct a descriptive account of the phenomena being

Table 1 Differences and similarities among the EU's GDPR, the USA's HIPAA, CCPA, GINA, and China's PIPL

	EU	The USA	China
Consent	It is explicitly defined as "freely given, specific, informed and unambiguous indication of the data subject's… agreement"	It does not explicitly define authorization	It is a significant concern. Handlers have to get consent, which can be revoked at any time
Sensitive information	It has specific categories, including "genetic data"	CCPA names genetic data as personal information and sensitive personal information	Open-ended examples (medical health, religion, financial accounts, etc.) It does not mention genetic data specifically but refers to the Personal Information Security Specification (PIS Specification) that mentions genetic data
Genetic data	Genetic data is considered "mostly" personal data; however partial genetic sequence used is not considered personal data if aggregated or anonymized	GINA is quite specific and comprehensive in regards to genetic data	PIS Specification says that specific personal and non-personal data must remain in China and cannot be accessed outside China, including genetic data. This is related to sharing and transferring of specific data
Legitimate interests basis	It includes an extra responsibility to protect individual's rights and interests in a legitimate interest assessment	It has exceptions for which individual authorization is not required	It does not exist
Automated decision making	Individuals can opt out unless carried out for legal or official authority or legitimate interest	CCPA, individuals can opt-out; HIPPA, consumers are notified about their data is going to be used	Individuals can opt-out. The decision-making has to be transparent
Facial recognition	It is considered a particular category of personal data under the GDPR since it makes it possible to identify a person uniquely. The 2018 privacy law prohibits processing such data unless there is explicit consent, a legal obligation, or public interest	It does not have a nationwide mandate. Every state decides for itself	It can be used only for public security reasons
Research use	It clarifies exceptions for research purposes	It clarifies exceptions for research purposes	It clarifies exceptions for research purposes

investigated" [48], fitting our main goal of evaluating practices on data protection and genetic data in the Turkish Health Information System. As participants interact and build on one another's comments, the researcher can generate large amounts of data describing, explaining, comparing, and evaluating a phenomenon. Moreover, through a facilitator, discussions can be probed for further details. Therefore, controversial, multifaceted, and multidisciplinary topics, such as genetic data privacy, benefit from it greatly. The purpose of the focus group session is not to arrive at an agreement on the investigated topics but to identify, understand, and sympathize with the stakeholder perceptions. Likewise, this study provides a discussion platform between experts and stakeholders to determine how genetic data is handled in Turkey based on their experiences and how the new legislation will bring insights into genetic data handling.

The participants were chosen with the purposive sampling technique, an expert sampling method. Experts are chosen to be research subjects [49]. In both focus group meetings, the participants of the host institute acted as the moderators. They introduced topics and guided the discussions.

The first focus group meeting lasted more than 2 h and included seven participants (three females, four males) and one moderator (female) from academia. Participants included two lawyers from an NGO overseeing the medical sector, a journalist in information technologies and society, an academic who specializes in cryptology and information security, an insurance company representative, a large IT company director for relations with the Ministry of Health, and an entrepreneur from a wearable devices company. The moderator was an academic specializing in genome sciences and informatics.

In the second focus group lasting 6 h, eleven participants (three females, seven males) discussed the collection of genetic data; discussions covered a wide range of topics on health information systems, ranging from electronic health records, comparisons of differences in the implementation of law in other countries to genomic data itself. The participants were representatives of NGOs (Turkish Medical Association, Bioethics Association, Medical Genetics Association, Patient Rights Association, and Medical Informatics Association), a data protection law consultant to a ministry, an industry representative from a genetic diagnostic center, and medical experts. Eight participants were academics specializing in medical genetics, clinical bioinformatics, or medical ethics. As these participants are experts in niche areas, thus easily identifiable, we refrain from providing more information about them in order to protect their anonymity. The moderator in the second focus group was the NGO lawyer hosting the meeting.

As the *main aim of the meetings* was to explore the experts' opinions on the regulations of the health information systems, data security, privacy, and confidentiality in Turkey, we examined important issues of the regulations of the health information systems from *legal*, *ethical*, and *security perspectives*, where implementation of the new *personal data protection (PDP) law* in Turkey on *genetic data* was investigated in further detail. The major topics addressed in both focus groups can be as follows:

- The Turkish National Health Information System (N-HIS) and the implementation of the PDP Law.
- E-Nabız's data access model as a mobile application serving national-wide electronic health records.
- Regulations allowing the Ministry of Health to centralize health data collection through N-HIS and E-Nabız.
- Regulations on protecting medical data regarding security, privacy, and confidentiality of the data.
- Genetic data management by healthcare givers and governmental institutes and respective PDP Law coverage of these practices.

This approach and the thematic broadness allowed us to draw on a rich corpus of data with interrelated links for this analysis.

Data Analysis

Both discussions were audio-recorded (permissions obtained verbally for the audio-recording) and transcribed for analysis with the participants' permission. In order to protect the participants' anonymity in the focus groups, codes were given, and feminine third-person pronouns were used for all participants.

A preliminary transcriptions analysis was conducted to understand the data and reflect on its meaning. The entire data set was organized, specified, simplified, and reduced. Then, the related parts were given separately and re-read, and essential elements were defined. Initial codes came together and turned into potential themes, which were organized. Our analysis of our focus group data revealed two main areas of concern: the lack of regulations governing access to and the handling of medical data and the management of genetic information in electronic patient records.

Findings

Insufficient Regulations for Access and Protection of Medical Data

Central Data Collection in Turkey

In both sessions, none of the participants were against the collection of health data; on the contrary, they believed that this collection was necessary, and concerns were related to the centralized storage and the anonymity of the data. As of the utmost concern, most interviewees demanded that health data be collected primarily to benefit each patient and society. However, the social and individual benefits depend on the "right methods" for storing and sharing data. So, encryption technologies should be effectively utilized to provide data privacy, security, and confidentiality for anonymity.

One participant underlines that the Ministry of Health already stores health data. So, the primary considerations are with whom, when, and under which conditions this data will be shared ("beyond the storage of the data, with whom and under which rules"). Although P3 (Private company director for relations with the Ministry of Health) is aware of the central organizational structure of the Ministry of Health, she emphasizes the importance of regulations on data privacy:

> "[W]hen it comes to confidential information such as patient data, I think that it can provide much help to find and propose rules and mechanisms such as security mechanisms, rules for sharing and evaluating, etc."

In other words, as the health data is already stored in central systems, implementing the data protection law is much more critical. The expert directly points out that rules and mechanisms for protecting patients and thus health data still need to be developed and implemented. This indicates that the implementation of the EU directives presented is insufficient. This will become clearer in the next section, especially about implementing the PDP law.

The Law Legalized Data Sharing

Many participants have a critical opinion on the legislation and wish it had never come into force, as unauthorized data collection "was a crime before the law came out, but now it is legalized. For the law makes it easy to capture and collect personal data, not to protect it; we have hesitations" (P1, NGO Lawyer). The lawyer P1 (NGO Lawyer) even thinks that the situation had been better before the PDP law was passed. Another participant from the second focus group had a similar view, stating that the PDP law legalized unauthorized access and gave the government special sharing rights (P4, Medical Genetics Academician). These concerns are related to two significant challenges of the law: excessive exceptions and data collection without consent in article 6, paragraph 3. Article 6, paragraph 1 defines the particular interest data as follows:

> "[R]elating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of an association, foundation or trade-union, health, sexual life, criminal conviction, and security measures, and biometrics and genetics are special categories of personal data." Article 6 – (1)

Although article 6(2) emphasizes the requirement for explicit consent by stating that it "is prohibited to process special categories of personal data without obtaining the explicit consent of the data subject" in paragraph 3, exceptions are listed that allow processing data categorized as special data without explicit consent [8]:

> "Personal data relating to health and sexual life can only be processed without obtaining the explicit consent of the data subject for purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment, and care services, planning and management of health services and financing by people under the obligation of secrecy or authorized institutions and organizations." (Article 6–3)

According to this paragraph, our participants pointed out that even data about patients' sexual orientation can be processed without the data owner's consent and that exceptions are challenging. P1(NGO Lawyer) criticizes:

> "There are too many exceptions. The bowl is uncovered, and the umbrella that protects it is too narrow. Hence the number of data subcategories unprotected by the law is more than the ones being protected."

P1 (NGO Lawyer) refers to article 6 paragraph 3 PDP, as it relates to circumventions of the legislation regarding collecting and processing sensitive data of individuals and institutions without their consent.

Another NGO lawyer, P10, pointed out that the PDP law gives this right to the Ministry of Health as well:

> "Within the same law, the Ministry of Health is also assigned the task related to collecting this data for certain purposes, like protecting public health, etc."

According to P10's (NGO Lawyer) claim, this part is added to the PDP law to legalize data collection of the e-Nabız system since it was suspended previously by the council's decision (November 2015). The decision suspended the collection and processing of the personal health data of the Turkish Ministry of Health in November 2015. The NGOs sued the Ministry of Health on the circular of e-Nabız in February 2015. Approximately, 9 months later, the council of state stopped the execution; hence, it stopped collecting and processing personal health data of the Ministry of Health [50].

The passage, which P10 (NGO Lawyer) mentioned, is article 47 [8], which is amended by the PDP law from the decree-law no 663 dated October 11th, 2011, on the organization and duties of the Ministry of Health.

P5 (Journalist) has similar concerns concerning the law's explicit consent as one of the most problematic parts. She explains this by referring to the third paragraph of Transitional Provisions, Temporary Item 1 [8],

> "that unless the data owner declared the opposite within one year, it is accepted that consent is given. It is not realistic for the data owner to remember whether she/he gave consent and when or where she/he gave it."

Exceptions defined in the law are highly criticized by the participants, even though the law was prepared based upon the Directive of the EU with high sensitivity to data confidentiality. However, the translation of the European Union directive numbered 95/46 is also a controversial topic. "The way of implementation" (P6, Data Protection Consultant of a Ministry) of the law and trust in the Turkish government are discussed under various titles in the meetings.

Previous Breaches of the Law by the Government

P1 (NGO Lawyer) remarks that the Ministry of Health does not obey the court decision, citing the case of e-Nabız as an example [51] and states that even though the court stopped the implementation of the application, it was still active:

> "When we look at health and safety, a very critical issue emerges. It should never be done before the legal infrastructure is established. After NGOs won the cases, they [e-Nabız, SaglikNet2, etc.] were all stopped by the court but actually continued. They never stopped completely."

NGO lawyer P11 emphasizes the importance of establishing a legal infrastructure; however, the unlawful acts were not stopped following the law's passing. The regulation of the protection of personal health information (numbered 29,863) was published by the Ministry of Health [52], and with the circular numbered 2016–6 about e-Nabız [53], the Ministry of Health started to collect health data again.

Two central problems of the regulation for the protection of personal health information are the following: one, data collection limitations since the NGO lawyers worry that with this regulation, every type of data could be collected and processed by government agencies.

> "There is no criterion of restricting by purpose, so the new regulation does not say that I want the following data for the following purposes. It says that when someone comes to you, you have to send me all of the data you have obtained from him." (P1, NGO Lawyer)

And two, starting the data collection prior to the establishment of the personal data protection board

(PDPB), which is regulated in article 47 (4) as the "Ministry shall take the necessary measures to ensure the safety of personal health data obtained under this law. For this purpose, it establishes a security system that allows controlling for what purpose the registered information is used by which officer." P1 (NGO lawyer)'s statement makes it clear that there was no establishment:

> "[T]he law stated that you can collect data only if you take the safety precautions prescribed by the personal data protection board (Article 47-Paragraph 4). However, the Ministry of Health would start to collect the data before the personal data protection board is established."

As NGO lawyers state, the article mentions the principles determined by the PDPB. The election of PDPB members [54] was completed on January 4th, 2017, about two and a half months after the regulation of the protection of personal health information was published (October 20th, 2016). P6 (Data Protection Consultant of a Ministry) accepts flaws within the regulations and indicates that the changes will be done soon.

Following a 5-month implementation period, changes to the regulation were made starting from November 24th, 2017 [55], as P6 (Data Protection Consultant of a Ministry) stated. Many of the contradictory paragraphs were updated or omitted from the modified regulation. Article 7 was one of those. Its former version allowed "authorized institutions and organizations" to process personal health data. In its second paragraph, it regulated that "in order for personal health data to be processed non-anonymously, except for the purposes listed in the first paragraph, the relevant person must be informed in detail regarding the reason for the disposal, the written consent of the person must be taken, and the consent must be stored." These contradictory paragraphs were modified as follows:

MODIFIED ARTICLE 7

1. No explicit consent of the person is sought for the personal health data to be processed under the exceptional purposes and conditions set out in the third paragraph of Article 6 of the Law.
2. To process personal health data within the scope of these purposes, the person must be informed, and consent must be taken according to the information provided in Article 10 of the Law.

Management of Genetic Information in Health Information Systems

Regulations and management of genetic data were the main topics at both group meetings. The discussion in the second meeting was concerned with the handling of genetic data. Genetic data is considered special data, as it differs from other data types in their unique features. Our participants stressed that the special character of genetic data, as it cannot be anonymized, is related to the family rather than the data owner alone and that it has the potential to generate more data about the owner in the future. These unique features of genetic data were discussed along with new legal developments.

The Distinction Between Genetic Data and Health Data

P6 (Data Protection Consultant of a Ministry) indicates that even though there is no article dedicated to it, there is no exception made for genetic data either, so it can be said that genetic data is under protection by the law:

> "In the first paragraph of article 6, apart from health data, biometric data and genetic data are counted separately. However, in the third paragraph, only sexual life and health-related data are mentioned as being exceptional. Therefore, it is obvious that genetic data cannot be processed [without consent] under 6/3." (P6, Data Protection Consultant of a Ministry)

Since this is the personal interpretation of P6 (Data Protection Consultant of a Ministry); the final decision would depend on the PDP Board.

The NGO lawyers agree with this view and add that according to the PDP law, genetic data cannot be processed without "any consent" of the subject (see P1), but "only if it is seen as health data." This statement is surprising as genetic data are often linked to health data and are considered as such. As genetic and health data are much intertwined, P8 (Representative of a Medical Diagnostics Center) points out that both types of data are difficult to distinguish from each other:

> "It is important to understand what is called genetic data. So clinically, I make the FMF

> diagnosis for a child. Does that health data become genetic data when I find the mutation? When will they be separated? Because apart from infectious diseases, 85% -90% of the remaining diseases are genetics-based. The discussion is so complicated at that point, so we should define very well what genetic data is and what is not."

Of relevance and possibly helpful would be a definition used by the health care system. Indeed, the Turkish Social Insurance Institution (SGK) does not define any differences between genetic and health data, while they are asking for information from clinics. A university medical genetics laboratory academic, P9 (Academician & Member of Medical Genetics Association), expresses that in practice, SGK is acting against the law:

> "In practice, we are producing the report; we are sending the bill to the SGK. The SGK tells us, 'what did you do to this patient and send me the 90 pages of the Sanger sequence. Put your signature on the detailed report below, send them to me, then I will put them in the patient file and then I will pay you the money'. When it comes to this point, then encapsulation or other technical measures seems very utopian."

P8 (Representative of a Medical Diagnostics Center) also reports that three members of the Medical Genetics Association have been investigated since the PDP law was published because they refused to report the whole genetic data with SGK.

Many respondents are aware of the sensitivity of genetic data and its implications. This is reflected in the discussion on whether genetic data can be separated from health data—and whether this involves genetic testing or the sequencing of an entire genome. In addition, genetic test results have two types of consequences: they can either provide a potential or an exact diagnosis. Specifically, this could be information about biological ancestry, disease disposition, and specific individual capabilities or life circumstances. In most cases, test results only offer probabilistic outcomes, and sharing these possibilities with patients is controversial. It is clear from the statements made by the respondents that these results can have severe and irreversible consequences if they are in any insurance company's hands. The particular sensitivity of genetic data also results from the fact that this type of information remains valid over long periods, statements could be made about future developments (predictive potential), and its significance could often be of considerable consequence for the life of the person—and the family—concerned.

Anonymization Does Not Work for Genetic Data

In the PDP law, genetic data is only listed under the special categories of personal data, but no article is predominantly dedicated to genetic data in law. However, P7 (Academician), who wrote several academic publications and research projects on the privacy and security of genetic data, reminded us that standard anonymization techniques would not be enough to protect the privacy of genetic information.

> "[I]n order to anonymize data, you should extract the personal identifier from it, but genetic data is a personal identifier itself."

P2 (Academician & Medical Informatics Association Representative) also addressed the same problem and added that only pseudonymization techniques could be applied to genetic data. ("genomic data cannot be anonymized (…). It can only be pseudonymized").

P6 (Data Protection Consultant of a Ministry) expressed thoughts similar to the academics' and added that while the law was prepared, they, as the Ministry of Health, presented their conclusion that the law must include pseudonymization for genetic data, as it is "absolutely essential for conducting clinical studies of scientific preparations or studies on genetic data because it is not possible to create anonymity." However, Turkish law does not mention the pseudonymization technique, although it was newly added to the GDPR (Recital: 26, 28, 29) [56, 57].

Anonymization by extracting the personal identifier from genetic data is not possible. Moreover, the unique properties of genetic data mean that it is related to more than one person; hence, the privacy of the data of a patient's family members should be considered while regulating the law.

Individual Consent May Not Be Enough

According to the participants, taking consent from the patients only is not sufficient since genetic data has far-reaching consequences for family members, as they would be affected by the results—lasting as "permanent knowledge." P4 (Medical Genetics Academician) justifies the difference in genetic data by stating that genetic diseases impact the patients' health conditions and their families. As the trans-individual meaning of genetic data goes beyond the "person's family, relatives, past, even future generations" (P2, Academician & Medical Informatics Association Representative), it may even include discriminatory elements. P2 (Academician & Medical Informatics Association Representative) explains:

> "If you define a person as a patient with a hereditary incurable disease, if you reveal this to society, that person and the whole family will be exposed to it. Discrimination can have very different effects at every level in society. And genomic knowledge is permanent knowledge, … So, if you do something [with the genetic code], you should take consent from the person's relatives, as well."

The interviewees indicated that genetic data has far-reaching consequences on all actors involved. These concerns also affect temporal dimensions and consequences regarding the manifestation of genetic knowledge. Interestingly, P2 (Academician & Medical Informatics Association Representative) speaks of immutable knowledge that, once spread, persists.

In this context, the absence of knowledge and the uncertainty in dealing with genetic information seem crucial as genetic research is still in its emerging phase. P2 (Academician & Medical Informatics Association Representative) underlines the difficulty of predicting what can be revealed and linked to genetic data. In this context, the risk cannot be estimated, and this includes the lack of knowledge about genetic data. Therefore, it is crucial to protect genetic data through laws, yet regulations in Turkey are, currently, not established for this purpose specifically (P2). P2 (Academician & Medical Informatics Association Representative) clarifies the economic importance of genetic data "beyond health" as a socially stratified good. These are essential and still controversial aspects of handling genetics in other countries. However, the fundamental problem of separating genetic data from health data was, nevertheless, being discussed in the meetings on the PDP law.

Discussion and Conclusion

There is a correlation between effective legislation and awareness among practitioners [44]. Studies on awareness of GDPR [58] and GINA [59] found that the knowledge on them is stratified among the population, and their potential has not been fulfilled yet. (PIPL is new, and to our knowledge, there has not yet been any study on its awareness.) Even though we have not explicitly conducted a similar study for Turkey, the focus group discussions have arguably shown that the situation in Turkey is similar. People with higher education and incomes are more sensitive to these issues, and the remaining population is disinterested.

Recently, an increasing number of people have expressed concern about the privacy of their information [60]. Nevertheless, many experts agree that the problem of public concern about security and privacy can be overcome through technical and regulatory changes [61]. Surprisingly, the participants' opinions about new legal actions in Turkey contradict this view. Some participants even find that the situation has worsened following the introduction of the PDP law. None of the participants in either meeting oppose data collection; however, they do not support the current way. They criticize the absence of legality while also being dissatisfied with the current law and regulations. There is a link between effective legislation and awareness among practitioners [44].

The participants claim that the system in Turkey aims to carry out a centralized data collection (as in the case of e-Nabiz), and the PDP law was designed to support this aim. According to their views, this is unacceptable since it is detrimental to data privacy, mainly because of the considerable data leak risks. Although decentralized health systems cause heavy expenses and many challenges [62], unauthorized access and abuse risks are higher when collecting large-scale data [63]. Besides the breach risks, there is a lack of trust in the Turkish government regarding the selling of personal health data on purpose. This is due to the bad reputation of the SGK, as the central Turkish health care institution “sold personal health data to 5 companies (pharmaceutical industry, foreign companies) for 65,000 TL (about 30,000 USD in 2013)“ [64, p.210].[1] Breach risks exist for many projects in some way or another; however, trust can be improved by regulation through strong laws, especially for privacy issues. The Turkish government needs to take constructive steps to increase the penalties for data abuse, giving the subjects all rights over their data.

Respondents found some articles of the new law threatening personal privacy potentially. In doing so, they referred to the EU as a desirable directive. Even though the Turkish PDP law was based on EU Directive number 95/46/EC, it is not an exact translation. Recently, the EU Commission criticized the PDP law in their Turkey report, stating that “it is not yet in line with European standards” [9].

Moreover, Directive 95/46/EC was replaced with the EU General Data Protection Regulation (GDPR) on May 25th, 2018. The regulatory policies changed significantly with the GDPR[65]. Data collection and processing without consent, especially for sex life data exceptions, are the most criticized part of the PDP law. Contrary to the situation in Turkey, the GDPR strengthens the issue of explicit consent. Moreover, the sentence “It must be as easy to withdraw consent as it is to give it” is added to the GDPR [65]. However, Transitional Provisions Temporary Item 1 [8] makes giving and withdrawing consent even more complicated. Updating the law according to GDPR and simplifying the consent withdrawal may solve these points. Consent is a significant concern for PIPL [47, 66]. In that sense, the indifference of the Turkish public to the issue is most troubling.

As previously explained, the regulation of the protection of personal health information [52] was revised [55] after a discussion in which the lawyer (P6) pointed out the regulation’s mistakes and counterproductive aspects with the law. Since the changes occurred after the meeting, it was impossible to explore the focus group members’ ideas about these changes. However, to this date, there have been no lawsuits contesting these changes.

In general, the discussants complain about the government not paying the necessary attention to the legal aspects regarding genetic data. Indeed, contrary to Directive 95/46/EC [67], genetic data is included in the list of special categories of data in the PDP law. However, the participants think this is a crucial but not solely sufficient step to protecting the privacy of genetic data. According to them, specific features of genetic data should be considered prior to taking any action. For instance, genetic data cannot be anonymized, so a pseudonymization technique was proposed in the meetings. Many sources in the literature support the participants’ opinions that genetic data is a personal identifier and cannot be anonymized by extracting the personal identifiers [68, 69].

According to the GDPR, pseudonymized data remains personal data protected for direct identification (GDPR, Recital 26) [56]. In other words, unlike anonymous data, pseudonymized data can be attributed to a natural person by using additional information [56]. On the other hand, anonymization is an irreversible process that makes the data no longer identifiable, and the GDPR does not regulate anonymized data at all, as well as PIPL, but the latter does not offer details. Instead, the GDPR suggests keeping data in an unidentifiable form while not being used [70]. In the case of personal data that cannot be anonymized, the GDPR states users/rulers can act by making an anonymous/pseudoanonymous decision based on how fast/cost-effectively pseudoanymized data can be decrypted. This statement can be addressed as the principle of relative anonymity, and, nowadays, such decisions are seen as harmless in order to facilitate data for research and public service purposes with benefits being predicted higher than the risks. However, the recalling of previously shared data as soon as technology begins processing it at a low-cost level may not be possible in practice at this point and may cause disclosures over the data shared. We expect these disclosures will have a higher impact on genetic data as it is information-transferable between generations.

We must further consider the gap in the adaptation of technologies around the world, which creates a challenge for standardization of the criteria for relative anonymity.

[1] For the thematic-legal analysis, see: Dülger MV (2021) Sgk’nın Kişisel Sağlık Verilerini Satış Konusu Haline Getirmiş Olmasına İlişkin Mahkeme Kararının Kesinleşmesi Üzerine: Kişisel Sağlık Verileri Satılabilir Mi? (Upon Finalization of the Court’s Decision Regarding the SGK Making Personal Health Data the Subject of Sale: Can Personal Health Data Be Sold?). https://doi.org/10.2139/ssrn.3792242

Genetic/genomic information stored and shared electronically should be evaluated based on how it can be processed globally with today's most advanced technology. With the completion of large-scale population genome projects and the development of quantum computing infrastructures, the cost of "genetic data identification" decreases. As a result, even today, it would not be the best decision to call pseudoanonymous genome/genetic data "relatively anonymous," assuming that it would be challenging to decipher it technologically.

Even though our participants suggested using pseudonymization for genetic data, pseudonymization would not be solely sufficient to share genetic data with second parties. Moreover, pseudonymization remains a debatable subject among the authorities since the GDPR's release due to the uncertainty of pseudonymized data being truly personal [56]. As we witness in many different scenarios, we have slow and weak reflexes for implementing new international legal regulations and practices. Considering these constraints, instead of ignoring the risks by accepting genetic/genomic data as relatively anonymized, accepting it as pseudoanonymous from the start can help us be aware of the risks, control the shared persons/institutions, and inform them about their responsibilities for undesirable events. Most importantly, we can focus on optimizing the prevention protocols today rather than delaying the problems on the horizon.

A family consent option needs to be discussed further within the scope of the law since disclosing this information may also have significant effects on the family members [71, 72]. The family consent issue is, in fact, discussed in the literature. Minari et al. [73] mentioned the benefits of family consent besides its technical, financial, and social challenges. Geneticists thought these challenges brought too much control over genetic research, so they opposed the idea [72]. However, many of these challenges can be overcome using Information and Communication Technologies [73].

Furthermore, it is not foreseeable that genetic science will develop in the future, and preventing genetic data from being stored in unsafe environments is crucial. We see family consent options as part of ethics for technologies that converge at the nanoscale.

Turkey's lack of specific legislation on genetic data is considered the most significant shortcoming. As the analysis by Joly et al. [29] showed, genetic discrimination exists, and people are concerned about it. Therefore, more detailed and constructive regulations are needed in this area, especially concerning vulnerable groups. GINA is one of the good examples proposed in the group meetings, but it is still criticized since it protects the privacy of genetic data only in the event of the patient actually developing symptoms [74]. An improved particular act to prevent genetic data from being abused in the insurance sector should be discussed in Turkey. Joly et al. also reported that identifying the genome could cause discrimination, especially by insurance companies [29]. The Turkish constitution is based essentially on the prevention of discrimination. No addition to the constitution may be needed, but a particular act might guarantee that misuse will be avoided.

On the administrative and regulatory level, collecting health and genetic information is not a problem unless it is not centrally collected, managed, processed, and accessible- without the data owner's consent. The new Turkish personal data protection law is problematic as the frame of collectible data is wide-ranging, and the exceptions are extensive. The importance of data owner consent is ignored even for sensitive data. Data about sex life can be collected to such an extent that almost everything can be included. The regulation was published after the PDP law received much negative feedback from the participants. There is no limitation on the data collection, so all kinds of data are wanted for collection.

Genetic data has many properties that should be considered while the laws and regulations are written. Although the genetic code is unique for every person, genetic illnesses are related to all family members. Therefore, when it is shared, it will affect other people besides the patient. There is also no possible way to get it back since genetic codes cannot be changed. Hence, the actions must be taken much more rigorously before collecting genetic data. Even though the new PDP law separated genetic data from health data, it was collected as health data by the government agency, SGK. Even the government investigated the people who tried to apply the law and refused the request. There should be specific laws or articles dedicated to genetic data that also overlook the dimension of discrimination based on genetic differences in Turkey.

Problems in the intersection of medicine, ethics, and law arise from increasingly specific findings in medical research and their application to patients. As specific and individual as applications on the nanoscale may be, the socio-ethical consequences for various areas of life (health, work, etc.) of the individual, their relatives, and even health policy itself are far-reaching. In addition to ethical aspects, economic and legal aspects of health should be included in the discussion to be carried out within the framework of socio-political analyses with culture-specific approaches and cross-culture boundaries simultaneously.

Acknowledgements The authors would like to thank those who were available for the focus group discussions. The authors would like to extend their gratitude to the anonymous peer reviewers for their careful reading, thoughtful comments, and efforts towards improving this article.

Funding Open Access funding enabled and organized by Projekt DEAL.

Data Availability The authors declare that the data supporting the findings of this study are available within the article. Due to ethical concerns, other supporting data cannot be made openly available.

Declarations

Conflict of Interest The authors declare no competing interests.

References

1. EU Directive (1995) Directive 95/46/EC of the European Parliament and of the Council 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. Off J Eur Comm 38(281):31–50
2. EU Commission (2003) First Report on the implementation of the Data Protection Directive (95/46/EC). Report from the Commission. COM (2003) 265 final, 15 May 2003. [EU Commission - COM Document]. https://op.europa.eu/en/publication-detail/-/publication/ff783aa5-5770-42e8-bac3-917fe0a361d7. Accessed 13 Mar 2022
3. Guinness World Records (2009) Most translated document. https://www.guinnessworldrecords.com/world-records/most-translated-document. Accessed 13 Mar 2022
4. Andrews EL (1998) European law aims to protect privacy of data. https://archive.nytimes.com/www.nytimes.com/library/tech/98/10/biztech/articles/26privacy.html. Accessed 13 Mar 2022
5. EU GDPR Portal (2017) Key changes with the General Data Protection Regulation. https://www.eugdpr.org/the-regulation.html. Accessed 15 May 2018
6. Greenleaf G, Laws GDP (2021) despite COVID delays, 145 laws show GDPR dominance (February 11th, 2021). (2021) 169 Privacy Laws & Business International Report, 1, 3–5. UNSW Law Research Paper No 21–60:6–19. https://doi.org/10.2139/ssrn.3836261.AccessedMarch13th2022
7. Fromholz JM (2000) The European Union Data Privacy Directive. Berkeley Technology Law Journal 15(418):461–484. https://doi.org/10.15779/Z383D48
8. Republic of Turkey (2016) Kişisel verilerin korunması kanunu. Resmi Gazete. https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf. Accessed 13 Mar 2022
9. Raul AC (2014) The privacy, data protection and cybersecurity law. Review Law Business Research
10. European Commission (2018) EU Turkey 2018 Report. Strasbourg
11. Ayday E, De Cristofaro E, Hubaux J-P, Tsudik G (2013) The chills and thrills of whole genome sequencing. Computer (iv):1–1. https://doi.org/10.1109/mc.2013.333
12. McGuire AL, Fisher R, Cusenza P, Hudson K, Rothstein MA, McGraw D, Matteson S, Glaser J, Henley DE (2008) Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: Points to consider. Genet Med 10(7):495–499. https://doi.org/10.1097/GIM.0b013e31817a8aaa
13. Alahmad G, Hifnawy T, Abbasi B, Dierickx K (2016) Attitudes toward medical and genetic confidentiality in the Saudi research biobank: An exploratory survey. Int J Med Informatics 87:84–90
14. Ayday E, Raisaro JL, McLaren PJ, Fellay J, Hubaux J-p Privacy-preserving computation of disease risk by using genomic, clinical, and environmental data. In: USENIX Workshop on Health Information Technologies, Washington DC, 2013. USENIX Association,
15. Gutmann A (2014) Privacy and progress in whole genome sequencing. Washington, D.C. doi:https://doi.org/10.1515/jwiet-2014-0119
16. Hoffman S (2017) Big data's new discrimination threats: Amending the Americans with Disabilities Act to cover discrimination based on data-driven predictions of future disease In: Cohen G, Hoffman A, Sage W (eds) Big data, health law, and bioethics. (Case Legal Studies Research Paper No. 2016–38). Available at SSRN: https://ssrn.com/abstract=2884317
17. Carroll JK, Moorhead A, Bond R, LeBlanc WG, Petrella RJ, Fiscella K (2017) Who uses mobile phone health apps and does use matter? A secondary data analytics approach. J Med Internet Res 19(4):e125. https://doi.org/10.2196/jmir.5604

18. Joly Y, Ngueng Feze I, Simard J (2013) Genetic discrimination and life insurance: A systematic review of the evidence. BMC Med 11(1):25–25. https://doi.org/10.1186/1741-7015-11-25
19. Mohammed S, Lim Z, Dean PH, Potts JE, Tang JNC, Etheridge SP, Lara A, Husband P, Sherwin ED, Ackerman MJ, Sanatani S (2017) Genetic insurance discrimination in sudden arrhythmia death syndromes. Empirical evidence from a cross-sectional survey in North America. Circ Cardiovasc Genet 10(1):e001442
20. Jones B (2012) Genetic Information Nondiscrimination Act of 2008 (GINA). Municipal Technical Advisory Service (MTAS), University of Tennessee
21. Council of E (2016) Recommendation CM/Rec(2016)8: On the processing of personal health-related data for insurance purposes, including data resulting from genetic tests
22. Kramer M (2016) Genetic discrimination: Transatlantic perspectives on the case for a European-level legal response. Disability & Society 31(1):141–143. https://doi.org/10.1080/09687599.2015.1075951
23. Frey L (2012) New directions in group communication. SAGE Publications. https://doi.org/10.4135/9781412990042
24. Etikan I (2016) Comparison of convenience sampling and purposive sampling. Am J Theor Appl Stat 5(1):1–4
25. T.C Danistay Onebesinci Daire Baskanligi (2015) Sağlık Bakanlığı'nın e-Nabız Projesi konulu genelgesinin iptali ve yürütmesinin durdurulması (2015/2900). https://www.ttb.org.tr/images/stories/haberler/file/danistay_10_daire_2015_karar.pdf. Accessed 13 Mar 2022
26. Türk Tabipleri Birliği (2016) e-Nabız Projesinin yürütmesi durduruldu. https://www.ttb.org.tr/975yccb. Accessed 13 Mar 2022
27. T.C Sağlık Bakanlığı (2016) 2016/6 Sayılı Sağlık.Net Online ve e-Nabız Genelgesi. https://sbsgm.saglik.gov.tr/Eklenti/820/0/genelge20166pdf.pdf. Accessed 13 Mar 2022
28. Kişisel Verileri Koruma Kurumu (2017) Kurumsal Tarihce. https://www.kvkk.gov.tr/Icerik/2075/Kurumsal-Tarihce. Accessed 13 Mar 2022
29. Kişisel sağlık verilerinin işlenmesi ve mahremiyetinin sağlanması hakkında yönetmelikte değişiklik yapılmasına dair yönetmelik (2017) T.C. Resmi Gazete (30250, 24 November 2017). https://www.resmigazete.gov.tr/eskiler/2017/11/20171124-1.htm. Accessed 13 Mar 2022
30. Mourby M, Mackey E, Elliot M, Gowans H, Wallace SE, Bell J, Smith H, Aidinlis S, Kaye J (2018) Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. Comput Law Secur Rev 34(2):222–233. https://doi.org/10.1016/j.clsr.2018.01.002
31. Blackmer WS (2018) EU general data protection regulation. SecureDataService
32. Madden M, Rainie L (2015) Americans' attitudes about privacy, security and surveillance. Pew Research Center
33. Rainie L, Anderson J (2017). The fate of online trust in the next decade. https://doi.org/10.1111/j.1559-1816.2010.00671.x/full
34. Oderkirk J, Ronchi E, Klazinga N (2013) International comparisons of health system performance among OECD countries: Opportunities and data privacy protection challenges. Health Policy 112(1–2):9–18
35. Gerry Qc F, Muraszkiewicz J, Vavoula N (2016) The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns. Comput Law Secur Rev 32(2):205–217
36. Şahinol M (2021) eHealth applications in knowledge landscapes. In: Svalastog AL, Gajović S, Webster A (eds) Navigating digital health landscapes: A multidisciplinary analysis. Springer, Singapore, pp 193–221
37. Hallinan D, Friedewald M, De Hert P (2013) Genetic data and the Data Protection Regulation: Anonymity, multiple subjects, sensitivity and a prohibitionary logic regarding genetic data? Comput Law Secur Rev 29(4):317–329
38. Malin BA (2005) An evaluation of the current state of genomic data privacy protection technology and a roadmap for the future. J Am Med Inform Assoc 12(1):28–34
39. Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y (2013) Identifying personal genomes by surname inference. Science 339(6117):321–324
40. Kişisel Sağlik Verilerinin Işlenmesi ve Mahremiyetinin Sağlanmasi Hakkinda Yönetmelik (2016) T.C. Resmi Gazete (29863, 20 October 2016). https://www.resmigazete.gov.tr/eskiler/2016/10/20161020-1.htm. Accessed 13 March 2022
41. Philips M (2018) Can genomic data be anonymised? (EU General Data Protection Regulation (GDPR) and Sensitive Research Data.) GA4GH Regulatory & Ethics Workstream (REWS)). ELIXIR. https://elixir-europe.org/documents/gdpr & https://www.ga4gh.org/news/can-genomic-data-be-anonymised/. Accessed 1 May 2020
42. Caulfield T (2002) Genetics, family consent and the law. Nat Rev Genet 3(9):647–647
43. Wadman M (2000) Geneticists oppose consent ruling. Nature 404(6774):114–115. https://doi.org/10.1038/35004731
44. Minari J, Teare H, Mitchell C, Kaye J, Kato K (2014) The emerging need for family-centric initiatives for obtaining consent in personal genome research. Genome Medicine 6(12):118–118
45. Molteni M (2019) The US urgently needs new genetic privacy laws. WIRED. https://www.wired.com/story/the-us-urgently-needs-new-genetic-privacy-laws/. Accessed 1 Oct 2020
46. Hoffman S (2016) Electronic health records and medical big data. Cambridge University Press, New York
47. Kohane IS (2011) Using electronic health records to drive discovery in disease genomics. Nature Review Genetics 12:417–428
48. Behrman RE, Benner JS, Brown JS, McClellan M, Woodcock J, Platt R (2011) Developing the sentinel system—a national resource for evidence development. N Engl J Med 364(6):498–499
49. Bragazzi NL, Dai H, Damiani G, Behzadifar M, Martini M, Wu J (2020) How big data and artificial intelligence can help better manage the COVID-19 pandemic. Int J Environ Res Public Health 17(9):3176
50. Raghupathi W, Raghupathi V (2014) Big data analytics in healthcare: Promise and potential. Health Information Science and Systems 2(1):1–10
51. Dimitrov DV (2016) Medical internet of things and big data in healthcare. Healthcare Informatics Research 22(3):156–163
52. Jonsson H, Luyolo M (2019) Revenue generation in data-driven healthcare: an exploratory study of how big data solutions can be integrated into the Swedish healthcare system;

https://www.diva-portal.org/smash/get/diva2:1334866/FULLTEXT01.pdf

53. Moore W, Frye S (2019) Review of HIPAA, Part 1: History, protected health information, and privacy and security rules. J Nucl Med Technol 47(4):269–272
54. Alder S (2022) What is protected health information?; https://www.hipaajournal.com/what-is-protected-health-information/. Accessed 5 Jan 2022
55. 中华人民共和国个人信息保护法 (Personal Information Protection Law of the People’s Republic of China), 中华人民共和国个人信息保护法_中国人大网 (npc.gov.cn). Accessed 10 Jan 2022
56. Komnenic M (2021) PIPL: China’s personal information protection law, China’s New privacy law. The PIPL explained. Accessed 10 Jan 2022
57. Spector-Bagdady K, Shuman AG (2018) Regent within the learning health system. Otolaryngology. Head and Neck Surg 158(3):405–406
58. Tanner A (2017) Our bodies, our data: How companies make billions selling our medical records. Beacon Press, Massachusetts
59. Abel S, Tsosie K (2019) Family history and the global politics of DNA. International Public History 2(2):20190015; https://doi.org/10.1515/iph-2019-0015
60. Terry NP (2017) Regulatory disruption and arbitrage in healthcare data protection. Yale J Health Policy Law Ethics 17:143–208
61. Price WN 2nd, Kaminski ME, Minssen T, Spector-Bagdady K (2019) Shadow health records meet new data privacy laws. Science 363:448–450
62. GDPR.EU (2022) What are the GDPR fines? https://gdpr.eu/fines/. Accessed 26 Jan 2022
63. Tessian (2022) 30 biggest GDPR fines so far (2020, 2021, 2022). https://www.tessian.com/blog/biggest-gdprfines-2020/. Accessed 29 Jan 2022
64. California Civil Code (2018) The California Consumer Privacy Act of 2018. Cal. Civ. Code § 1798. https://theccpa.org/. Accessed 21 Jan 2022
65. McCoy MS, Joffe S, Emanuel EJ (2020) Sharing patient data without exploiting patients. Journal of the American Medical Association; doi:https://doi.org/10.1001/jama.2019.22354
66. Koeninger K, Bradshaw R, Hinson PA, Conley (2020). International health data: How HIPAA interacts with the EU GDPR. https://www.robinsonbradshaw.com/media/publication/657_International%20Health%20Data.pdf
67. Joly Y, Dupras C, Pinkesz M, Tovino SA, Rothstein MA (2020) Looking beyond GINA: Policy approaches to address genetic discrimination. Annu Rev Genomics Hum Genet 21(1):491–507
68. Moneer O, Miller JE, Shah ND, Ross JS (2021) Direct-to-consumer personal genomic tests need better regulation. Nat Med 27:940–943
69. Ustaran E (2019) European Data Protection Law and practice. Second edition. The International Association of Privacy Professionals (IAPP)
70. Kaplan CS (1998) Strict European privacy law puts pressure on US; https://archive.nytimes.com/www.nytimes.com/library/tech/98/10/cyber/cyberlaw/09law.html. Accessed 13 Mar 2022
71. R Rughinis C Rughinis SN Vulpd D Rosner 2021 From social netizens to data citizens: Variations of GDPR awareness in 28 European countries Comput Law Secur Rev 42 https://doi.org/10.1016/j.clsr.2021.105585
72. Lenartz A, Scherer AM, Uhlman WR, Suter SM, Hartley CA, Prince AER (2021) The persistent lack of knowledge and misunderstanding of the Genetic Information Nondiscrimination Act (GINA) more than a decade after passage. Genet Med 23(2):2324–2334
73. Greenleaf G (2021) China’s completed Personal Information Protection Law: Rights plus cybersecurity. Privacy Laws & Business International Report. https://doi.org/10.2139/ssrn.3989775
74. Ghathakurta, R. (2022). A brief note on China’s Personal Information Protection Law. IndraStra Global; https://nbn-resolving.org/urn:nbn:de:0168-ssoar-78120-2

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.