CHAPTER 12

PRIVACY FOR ENTERPRISES IN THE DATA AGE

Bilgin METİN* Enes YILMAZ*, Erdi ŞEKERCİLER*

*Bogazici University, Department of Management Information Systems, Istanbul, Turkey
e-mail:bilgin.metin@boun.edu.tr

DOI: 10.26650/B/ET06.2020.011.12

Abstract

The world we live in is now becoming increasingly virtual. We all interact with this new age which we can describe as the digital age. We shop online, we communicate with people via social media, we are informed at any time through the devices that are in our hands about goings-on, whether we like it or not, we have become a part of this globalized and digitalized world. Data can be described as the structure of the digitalized world. In each interaction between us and the tools which we use, we create data or we cause data transferring or we can be a small part of a large data collection because of our presence in a platform on the internet. Certainly, this close relationship can reveal our private life in some situations. Most of the time, we are exposed to situations where our private information is collected, used, and processed without our permission. Sometimes we cannot even notice the violation of one of the most fundamental rights and freedoms we can define as privacy. This literature survey study is based on the fundamentals of information security, and it seeks answers to these questions: Why does our personal information need protection? What kind of information should be protected? What is the situation regarding the data privacy in Turkish and world law? What kind of laws have been passed upon the privacy of tax from past to today? What are the perspectives, opinions on protection of personal data in Turkey and Europe? What is the importance of data privacy for the business sectors? We also believe that this study will raise awareness on this matter.

Keywords: Privacy, Cyber security, Digital transformation

Introduction

1. What is Privacy? and Why We Need It

In today's digital world, the meaning of treasure has changed. 100 years ago, the notion of treasure was gold, petrol or maybe being a landowner. The transformation of the world in the last decades has affected our values, our standards, and concepts. Today, there are more valuable things than gold or petrol. Today's treasure is data (deMontjoye, Wang, Pentland, Anh & Datta, 2012).

Almost all the enterprises, institutions in various sectors such as the finance sector, health sector, energy sector use modern computerized techniques for digitalization based on collecting data. We are used to interact with these information systems every day. For example, while shopping, and in the hospitals, our personal information is collected. While we download a smart phones application, some personal access permissions should be allowed. While popular applications of digital life such as mobile banking, e-commerce, mobile signature, etc. make life easier for us, they let public or private organizations to observe our data. Companies, banks, hospitals, and government institutions log our behaviors, movements and store our private data, but they are expected to be careful and respectful of the privacy.

Privacy is one of the fundamental rights included in most of the contracts, agreements and countries' constitutions (Dülger, 2018). It aims to protect information which defines who we are, what we do, what we think and what we believe (Bignami, 2007), (Dumortier & Goemans, 2000). Privacy/Confidentiality keeps information that is conducted from data processing or correspondence between involved parties during an operation wanted to be hidden from unrelated third parties. Privacy creates a strict line between our personal life and the world, so it provides personal freedom/liberty and self-respect by blocking excessive interference of others. McFarland (2012), and Phelps et al. (2000) emphasize that privacy is a term that contains four dimensions: (1) intrusion (invading a person's loneliness), (2) disclosure (publicly revealing private facts), (3) false light (false public portrayal) and (4) appropriation (using personal identity without permission). If our privacy is protected, we have control on who has access to our personal life, such as our secrets, locations, telephone number and credentials. We can reduce publicly known private information and protect this information from unauthorized/illegal use of power as a consequence of privacy (Wagner DeCew, 1986).

Technology has improved dramatically in the last two or three decades, with the Internet becoming an important part of our lives. We witness novel technological infrastructures and devices, like IoT improved with the help of modern information technology systems such as ERP and cloud systems every passing day. With these technological improvements, the world has become more and more connected and digitalized, enabling people and organizations to reach their data from anywhere easily and collect others' information with new systems and applications (Chiper Cloud, 2015).

New technological devices and applications provide an opportunity to collect other people's personal information without their knowledge. For example, most of the people use smart devices like mobile phones, and some applications and features provided by them such as messages, shopping online, Google search, and calendar tasks. It is impossible to keep pace with the digitalizing world without using one of these functions. In normal circumstances, people set passwords to their devices in order to protect personal information confidentiality (Hoven et al., 2014). However, many powerful organizations such as Google and Facebook collect vast amount of information about us like location, profile, financial data, habits, e-mail, health situation, psychometric and political interests. Even if all this information such as political interest or health situation is not collected directly, this data can be obtained by combining different data collected via cookies. Therefore, it can be said that our control is low over which information is collected about us (de Montjoye et al., 2012).

With new laws, technologies and leaked information, the government has legal power to watch not only terrorists, but also all citizens. This monitoring activity encompasses call records/history, internet surfing, e-mails, social networking accounts, etc. (Bignami, 2007; Privacy International, 2016). Also, some powerful organizations bend the law in order to collect our private information. This situation causes a debate about an individual right to privacy versus the financial interest of corporations and the security concerns of government. Even worse, although people are the main related party, they barely know this issue because it is conducted in a confidential manner. Companies push the limits of the law regarding processing personal data in order to gain extra benefits, such as increasing their profit and the number of active customers. Companies need to offer their customers more customized campaigns and opportunities than other companies to be able to achieve this goal. Taking into consideration the fact that companies need even a piece of information related to a particular person, and sole information or anonymized information are useless to provide personalized offers, they need to monitor, brand, categorize and profile this data (Privacy International, 2016).

Technological developments have a lot of advantages for people and organizations, taking into consideration the fact that they make our lives easier. However, they also carry high risk potential when taken into account the increasing number of cyber-attacks to corporations like banks and telecommunication companies which have huge amounts of valuable personal data including individual's name, address, social security number, date of birth, alien registration number, taxpayer identification number, government passport number, driver's license information, mother's maiden name, or biometric information. This data can be used for identity theft, which is one of the popular cybercrimes in the digitalizing world (Chiper Cloud, 2015), (Allison et al., 2005).

Businesses using consumers' personal information may lead to competitive advantages over other companies. For example, financial data, search background in the company website, and purchase habits, are used to provide a better and targeted service (Dülger, 2019a). However, they also use this information out of their business scope. Note only businesses, but with the help of new technologies, now everyone can collect personal data. Since everyone gathers data, everyone can become a potential target, and this situation negatively affects the data privacy. Therefore, data security is a subject that needs to be argued, and we should make a distinction between data security and data privacy. These two are used as synonyms, however, these are just related concepts. Data security is a policy to ensure data privacy. Data security is about the confidentiality, availability and integrity of data, namely, it keeps data accurate and reliable, and it contains processes and implementations to ensure the data is not used by unknown individuals (CSX, 2015). Data security is also engaged in making plans, that is, gathering required information, keeping information and deleting information, so it helps to obey the legal restrictions. As for that, data privacy is the usage of data in an appropriate way. There are some legal obligations about data privacy. For example, usage of private information must be on an agreement with a company and the owner of the information. The information also cannot be sold and disclosed without permission. Therefore, industries, enterprises or individuals working with data must have a real data security policy to provide privacy of the data. When we provide a lot of personal data to these companies and other third parties, unwarranted disclosure of the data has the potential risk to be victim of cybercrime (O'Brien, 2019).

Some important companies have been hit with a series of security breaches over the past year. For example, the cyberattack on the Marriott hotel chain that collected personal details of roughly 500 million guests was exposed (New York Times, 2018). Furthermore, more than 540 million records of Facebook users were publicly exposed on Amazon's cloud computing

service. It exposed 146 gigabytes of Facebook user data, including account names, IDs and details about comments and reactions to posts (CBSnews, 2019). The main cause of this catastrophic result is unauthorized disclosure of personal information. This event increases public awareness about the importance of protecting privacy information, and people start to put pressure on the government and organizations to protect their personal information (Pascual, Marchini & Miller, 2016).

As a result of this, when we consider all these issues, privacy of personal data is not a need; it can be thought as a necessity or even an essential right regarding people, government and organizations. Therefore, a government introduces a wide range of legislation and regulation to create a balance between protecting private information and providing better service. Considering businesses reputation and trustworthiness, they also give adequate impotence to the privacy issue, so every company must develop and apply strong privacy policies and procedures (International Telecommunication Union, 2006).

2. Privacy of Personal Data in Law

Personal information has had an important place in the EU for a long time. The beginning of the data protection law can be seen in the European Convention on Human Rights which is an international agreement signed in 1950 related to the protection of private information. According to this agreement, people show respect to others' personal life, and no one can interfere with personal life except in the case of legal and democratic issues. With the advent of new technological developments, an agreement which protects individuals from processing their information automatically, was prepared in 1981. Turkey also signed this agreement to build good a relationship with EU countries (Ersoy, 2007), (Keser et al., 2014).

In the 1970s, governments used database systems to store citizens' personal information. Western European States, notably Germany, had some unpleasant experiences related tostoring and processing of personal data limitlessly (Küzeci, 2010). The first legal act considering the data protection of private data started to be implemented in the 1970s. This law mainly focuses on government establishment and some private sector organizations such as telecommunication and banks which collect confidential information of people. However, police forces/ law enforcement were outside of the scope of the law because of national security issues, so there is no restriction for the legal power to collect and monitor personal information of the citizens (Bignami, 2007). During these years, similar laws were applied in the US. The law named Fair Information Practice Principles (FIIPs) played an important role in creating privacy lines in the US in different areas, such as Health, Education and Wealth,

and also in other countries (Solove & Hartzog, 2014). In addition to these countries, Turkey also came up with the Central Population Administration System project (CPAS), which was created in 1973, and became effective in 2002. Protecting and using personal data in accordance with the purpose of collecting data can be one of the most important applications performed in this area (Ersoy, 2007).

After the advance of the internet and the development of new technologies, people have shared a lot of information in the online environment; therefore, in any criminal situation, police can use this information such as phone calls, cameras, and traffic data to locate or identify us. Considering the fact that we no longer live without using new technologies, countries have created new regulations, directives or acts which, to some extent, control the private sector, government and law enforcement.

In Europe, a second law related to data protection was the Data Protection Directive, that is the first legal act which was prepared in 1990, and became effective in 1995, to protect personal information (Bignami, 2007). The directive covers private organizations and Government Corporations which serve citizens by using their private information in order to prevent the illegal use of personal information (Bignami, 2007). The directive's main purpose is to create a common standard between EU countries considering data processes (Keser et al, 2014). Turkey has also performed similar studies about data protection during these years. When the related Commission did not complete the draft related to processing personal information automatically, the Ministry of Justice sent the Protection Personal Data Law which was prepared again, to relevant Ministries, and new resolution was sent to the prime minister's office in 2004. This resolution included a common application applied all around the world related to the Data Protection Law (Ersoy, 2007). With the 12th of September, 2010 plebiscite, a provision was added to article 20 of the constitution. According to this law, everybody has a right to have protection of personal data. Usage of this data depends on the permission of the owner of the data (Turan, 2016).

Data privacy issues have increased after the spread of the Internet and the development of new technologies like smart-phones, IoT devices, etc. New technological improvements make the data gathering, sharing, and analyzing processes easier so organizations have a substantial amount of information (Ersoy, 2007; Keser, et al., 2014). This situation makes organizations the targets of cyber criminals/hackers, and naturally, the number of cybercrimes related to data protection privacy increases (Ersoy, 2007). According to Hewlett Packard (HP) research, the number of cyber-attacks occurred in 2011 increased by 56%, and 86% of web applications are not safe, considering inscription and interface issues. Also, Symantec

research shows that cyber criminals produce more malicious code, viruses, etc. to get information from the online environment (Henkoğlu & Yılmaz, 2013).

Considering new coming threats, the Data Protection Directive which was signed with the EU, was not reliable anymore because every single country in the EU can adjust these directives according to their domestic law. Therefore, there is a need for a more common and widely accepted regulation. In 2012, the European Concil issued a new regulation applied in all the EU countries in the same way. In Europe, the protection in question is provided with two systems. The first one is the European Council. At the level of the Council, protection is provided by the European Convention on Human Rights article 8 and Section 108 of the Agreement: Right to respect for private and family life, home and correspondence. According to this Agreement, personal data should be:

- Fair and collected legally
- Collected for legal purposes and used for this purpose
- Relevant and sufficient, should not be exceeded
- Accurate and current
- Kept as long as necessary according to the collecting purpose (Dedeoğlu, 2004)

The second one is the General Data Protection Regulation (GDPR). The GDPR was adopted on 14 April 2016 from the Data Protection Directive 95/46/EC. The GDPR has been recognized as law, and became enforceable beginning on 25 May 2018.

In addition to this, in 2013, the EU stated that Turkey did not have a framework and appliance related to the privacy of personal data, and this situation had a negative impact on the relationship between Turkey and the EU (Keser et al, 2014). As a result of this situation, in 2016, the Turkish government accepted the data protection law in March 3, and published the regulation on April 07 (KVKK, 2016). With the law, the Protection of Personal data, scope, purpose and descriptions were clearly specified. Moreover, there are some principles of processes of data like deleting, destroying, anonymizing and transferring.

3. Privacy in Enterprises

The application of the personal data protection law differs in sectorial basis in some countries. Generally, many developed/developing countries such as the EU countries and Turkey use the same regulation or procedure for all sectors, so it provides a whole perspective (Strahilevitz, 2013), (Solove & Hartzog, 2014). Even though there are no sectorial rules and laws in this type of countries related to privacy concerns, governments establish different types of regulatory and supervisory authorities in order to determine the working principles of these sectors and market rules in general meaning, and enforce these conditions on specific sectors. For example, in Turkey, there is the Banking Regulation and Supervision Agency (BDDK), Capital Markets Board (SPK), Public Procurement Authority (KİK), Competition Authority (RK), Public Oversight, Accounting and Auditing Standards Board (KGMDSK), Energy Market Regulatory and Supervisory Authority (EPDK), Radio and Television Supreme Council(RTÜK), Information and Communication Technologies Authority (BTK), the Tobacco and Alcohol Market Regulatory Authority (TAPDK) and the Biosecurity Council (BK). These regulatory authorities are not for handling privacy concerns; they are just ensuring that these sectors do not act against the law within business processes (Çırakoğlu, 2016).

However, some countries like the US apply a different law and data protection act according to sectors. There are multiple laws and regulations related to how organizations protect the personal data of their customers. Although there are no laws and regulations which cover privacy of personal data, all organizations should follow their sectorial rules while they process personal data (Strahilevitz, 2013; Solove& Hartzog, 2014). This sectorial basis approach can be thought of as an inadequate application because of the lack of ability to see the whole picture, so in this approach, the country can have difficulties in taking immediate or real time actions in case of a new situation (Strahilevitz, 2013). Despite that, some others think that it is a good application of the data protection law because sector specific cases are handled easily by laws, and this type of regulation proposes customized rules and application methods for each unique sector (Nissenbaum, 2014; Schwartz, 2004). Some of the laws in force are the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach Bliley Act, the Fair Credit Reporting Act, the Privacy Act of 1974, the Telephone Records and Privacy Protection Act, the Electronic Communication Privacy Act, the Family Education Rights and Privacy Act, and the Payment Card Industry Data Security Standard.

For compliance with the related privacy laws, organizations should examine their risky personal data processing actions and focus on how to collect, maintain and process personal

data for mitigating or terminating these risks with a Privacy Impact Assessment (ISO/IEC 29134, 2017), (IPC, 2015), (ICO, 2015), (SEC, 2007), (HIQA, 2017).

3.1 Sectoral Appliance

3.1.1. Health

In the health sector, the usage of Information Technology (IT) is gradually increasing. Yu emphasized that Artificial intelligence (AI) is modifying medical practice using digitized data acquisition, machine learning and computing infrastructure. AI applications are expanding into areas that were previously thought to be only the province of human experts. (Yu et al., 2018)

The usage of IT provides organizations with using data more efficiently and in a meaningful way. In the US, using health data brings almost a $300 billion financial acquisition to this sector. (Kayyali et al, 2013). It does not just have a monetary advantage, but it also helps the health sector diagnose illness before the progression of the disease by using big data related to the history in the health records. Also, hospitals are connected to the same network, and doctors or physicians get a lot of information related to the same disease in order to apply the best treatment and early diagnosis, so they can have different perspectives and, if they miss something, they can capture the information by means of this system (Kayyali et al , 2013). A similar system, called epSOS (Smart Open Services for European Patients), is used in 12 EU countries (Linden, 2009).

In addition to this, the use of big data brings along a lot of developments in the medical field. For example, doctors suggest many hypotheses for the cure of different diseases. In order to find the right treatment method, they need more data and subject groups (Wang, 2018). Considering the fact that using patients' health data, which are private, has numerous advantages, it is not a surprise that the amount of information collected increases dramatically. For example, in 2012, the amount of health records in electronic systems to make data sharing easy increased from 30% to 75% (Keser et al., 2014). The increase of data sharing causes a dilemma between privacy of personal data and applying the best treatment. Therefore, governments establish some laws and regulations considering privacy concerns.

In some countries, there are specific laws related to the health sector, such as HIPAA for the US government. HIPAA basically creates limitations in sharing or using medical records collected via health providers such as hospitals and doctors. Some medical records cannot be transferred until the patient expresses consent. This law also allows health providers to keep

medical records in an electronic environment and ensures the protection of this type of data by conducting some security protocols. There is also some regional/ state legislation in order to protect health records (Solove & Hartzog, 2014).

3.1.2. Education

In education institutions, with the help of technology, the usage of data including personal data is quite high. The advance of online courses and technological applications make monitoring students and taking necessary actions related to students possible. Also, this type of education method will be useful for people with special needs. In the US, the Department of Education tries to prepare education plans by analyzing data which are collected via the online education program. In addition to this, online environment schools will able to examine teacher's performance, and this transparency will create a competitive environment so the problematic issue resulting from teachers' education methodology will be determined. As a result of this, the quality of education increases in parallel with the usage of personal data. In Turkey, there is a project called FATIH (Increase Opportunities and Technology Improvement Act). The main objective is developing an education system by analyzing students' data collected via tablet computers (Keser et al., 2014).

This type of data usage comes with the question of whether educators should collect and use data that identify students' or teachers' profiles. If data is transfered into an anonymized form, it will not be a problem, but in some situations, it can be used for different versions. Therefore, there are some laws related to this issue in almost all countries. In the US, this legislation is tied to a specific regulation called FERPA. This legislation mandates schools/ colleagues to inform students and their families in order to protect the privacy of education records. Thanks to this law, students review their records with respect to the accuracy of these records. Also, this law prevents students' records to be preserved, not only informal channels but also formal channels (Solove & Hartzog, 2014), (Walch, 2011).

3.1.3. Finance

In the finance sector, IT technology is used intentionally and collects a lot of public and personal information (Pendley, 2018). The use of IT technology and collecting personal data have a substantial amount of advantages in this sector, such as determining some fraudulent activities while analyzing the user's past habits. For example, if a user does not use his/her credit card abroad, and then someday, the user uses the credit card abroad for the first time, the bank informs the user about the expenditure and requires mobile or digital confirmation. Also, banks analyze users' data in order to offer specific promotions. With the help of this

data, banks predict some critical incidents, including problems occurring through economic crises, and they determine and take the necessary action before the incident takes place. In addition to this, they can calculate users' credibility, and determine which users are in high risk groups so they can save more money and make good investments. With the advent of mobile devices and applications, the amount of data collection has increased; therefore, analyzing users' patterns also increases and becomes more accurate. In parallel with the increase in data collection, some extra security measures are taken by authorities (Keser et al., 2014).

Cloud systems also have an important role in data collection and analyzing issue. However, in some countries like Turkey, although cloud systems are used in different areas, in the finance sector, there are some restrictions. BDDK mandates banks to hold their primary (main sources of the data are kept) and secondary (backup of the information system) systems domestically in order to keep their citizens information private. When we consider the importance and characteristic features of personal data used in the banking sector, this sector has a higher risk than others, considering cyber-attacks and the use personal data. Therefore, authorities legislate for this sector (Keser et al., 2014).

In the US, there are specific laws and regulations related to the finance sector different from the GDPR conducted in the EU. One of them is the GLBA, which covers legislations for the banking sector in order to protect customers' personal information, including financial data. According to this act, banks must inform their customers about privacy policies and procedures conducted within the bank. Also, this law provides customers with opt-out channels to some extent. Thanks to the opt-out channels, customers prevent banks from sharing their information with third parties (Code, 1999), (Solove & Hartzog, 2014).

The other law is FCRA, which covers some rules about both customers' financial information and credit information to prevent inadvertent disclosure. This law mandates banks to ask consent from their customers when sharing the financial information with third parties. In some situations, such as the processes of employment, this information is shared with some institutions (employers). Even if the user gives consent for sharing their information with third parties, employers also accept they will use this information within the scope of the legislation (Stokes, 1999).

3.1.4. Telecommunication

The intense usage of technological devices collecting personal data requires regulations and procedures for the purpose of protecting the privacy of people. In the telecommunications

sector, there is a lot of information relevant to customers such as personal information (ID, IP and address), traffic information (subscriber usage), bill information, location information, etc. Telecommunication companies use this information to provide better service to their customers, and access these people in case of an emergency using their location information. The data collected by these companies can include unnecessary information about the customer. In order to prevent this, authorities enforce some regulations. In Turkey, there is no specific law for this sector; however, there is the BTK, which protects customer's rights and information security in a general meaning (Onur, 2013).

In the US, there are the TRPPA and ECPA laws. TRPPA basically prevents telecommunications and similar companies from selling and sharing telephone records, call logs, etc., and applying monetary sentences to dissuade these institutions. There are some exceptions in the case of criminal cases for police forces (TRPPA, 2007). The other act is ECPA, which protects customers' information collected during transactions, storage such as e-mail, etc. in the electronic environment. The law mandates companies to obtain customers' consent in order to track their behavior and usage statistics (Solove & Hartzog, 2014).

3.1.5. Public/State

In public sectors, a substantial amount of data, including both public, like weather conditions and private, such as address information are collected by corporations (Aggarwal, 2019). In some countries, this information is shared with the private sector as open data in order to obtain financial earnings. However, this data sharing and processing must have some limitations and restrictions (Keser et al., 2014).

In the US, for federal agencies and public institutions, there is a specific law called the Privacy Act of 1974. With this law, the government provides protection to citizens with unauthorized disclosure of personal information compiled about a specific person by legal forces without permission of the people. Also, people are authorized to see their records in order to control whether their records are correct or not (Privacy Act, 1974).

3.2. Disclosure of Personal Information

Rapidly growing technology makes an enormous data warehouse available on the Internet. This warehouse also includes our personal information. For example, information on a Facebook account (Dülger, 2019b) almost equals the information that can be obtained by an intelligence agency with a long term study, through Twitter, it is possible to see where a person is, what he/she is doing, even what he/she is thinking (Küzeci, 2010). Some social

networking sites have more numbers than the population of most of countries. These sites provide an opportunity to access a person's information and photos, and to be seen by other people (Kılınç, 2012).

Undoubtedly, people accept to share their personal information, to record their speech and behaviors in order to make their life easier, increase their life quality and use their personal rights. This personal information can be stored, analyzed and spread. Besides, there is no way to know how this information is used. That is why the unauthorized disclosure of the information about private life arises (Kılınç, 2012), (İzgi, 2014). Various services offered on the Internet cause the disclosure of personal information publicly. Now, organizations have to take a stand against a wide range of risks and threats, like ways of e-fraud, information theft, hackers, information leakage, internal attacks, etc. (Karaarslan et al., 2010).

Rising risks and threats lead to security problems because personal information can only be declared, processed, stored and transferred within the permission of the owner of the information (Kaya, 2011). Although lots of organizations try to find a solution in terms of their perspectives, personal information can be released or stolen in many ways. Personal information can even be obtained by querying some information in the government's systems (Ketizmen & Ülküderner, 2007). Problems about the disclosure of personal information are controversial in the EU also. For example, in 2013, the disclosure of personal data of German citizens was obtained by the UK and the US intelligence agencies as one of the important propaganda materials of Merkel's opponents (Ceran, 2014).

Since information and communication technologies are commonly used in daily life, unauthorized disclosures of the information can be seen in many fields that are engaged in data, like banking, e-commercial, healthcare, education, etc. (Henkoğlu & Yılmaz, 2013). Some important private information can be gathered from various information sources. In addition to this, by using social engineering techniques, valuable information can be obtained (Ketizmen & Ülküderner, 2007). Although most of the organizations take some precautions against the leakage of information, there are deficiencies in the precautions. The most important deficiencies are firstly, technical factors and secondly, human factors (Henkoğlu & Yılmaz, 2013).

3.2.1. Classical (offline) identity theft: Identity thieves employ all kinds of methods to obtain personal data. One of the methods is parrying the security process, making use of human errors and social engineering. Influence, forcing, developing deceptive relationships can be counted as ways of social engineering. Other classical methods are dumpster diving, pretexting, shoulder surfing, skimming and business theft.

3.2.2. Online identity theft: These methods are unlimited because each passing day, a new one arises. The most important and common methods for online identity theft are:

- Malwares: Software that are installed into computers, mobile phones, and smart devices.
- Some deceptive e-mails and websites:
  - *Phishing:* Some e-mails that are disguised as coming from an enterprise, banks, government, or mirror web sites, namely a fake copy of a real website. These e-mails and websites are used for stealing users' personal information, like card information, passwords, etc.
  - *Spam:* Some e-mails come involuntarily and include harmful contents.

3.2.3. Hacking: It is another way of getting personal identity. By using hacking methods, personal information can be stolen through the system's gaps (OECD, 2008), (New York Times, 2018;) (CBSNews, 2019).

Abuse of personal data is another title for the disclosure of personal information. It is distributing and selling the commercial and occupational secrets to obtain an advantage. The data of banks, governments and hospitals have a commercially incredible value. Moreover, the release of this type of data can be a step for committing significant crimes (Karimi & Korkmaz, 2013).

4. Conclusion

Today, it is almost impossible for our information to be hidden behind closed doors. In every aspect of our lives, we encounter situations where information is recorded and used. Laws are the only regulatory factors that will prevent our personal data from being used without our permission.

With this study, we have revealed the examination of the law of data protection which has been enacted recently in our country, in terms of what its scope is, which situations are included, how it will be implemented, what it will bring, and so on. In terms of information security, this is a great development for our country to reach the standards of Europe in the data protection issue. In this context, the law on the protection of personal data, which removes many uncertainties and protects our privacy in the digital world, should be regarded as a milestone. Unfortunately, we should say that neither our people nor our organizations have the necessary and sufficient knowledge about this law and its benefits. Particularly, all

small and large organizations should be aware of this law and its sanctions. In this way, we can preclude the abuse of personal data. Although legal regulations for the protection of personal data are not strong enough to provide complete protection against rapidly evolving technology, it is the most important assurance we have to rely on.

Acknowledgement:

The authors thank Meltem Mutlutürk for her help writing the manuscript.

References

de Montjoye, Y. A., Wang, S. S., Pentland, A., Anh, D. T. T., & Datta, A. (2012). On the Trusted Use of Large-Scale Personal Data. *IEEE Data Eng. Bull.*, *35*(4), 5-8.

Bignami, F. (2007). Privacy and law enforcement in the European union: the data retention directive. Chi. J. Int'l L., 8, 233.

Dumortier, J., & Goemans, C. (2000). Data privacy and standardization. In CEN/ISSS Open Seminar on Data Protection, disponible sur https://www. law. kuleuven. be/icri/publications/90CEN-Paper. pdf.

McFarland, M. "Definitions of Privacy." Internet: www.scu.edu/ethics/focus-areas/internet-ethics/resources/what-is-privacy/, Jun. 01, 2012 [Oct. 06, 2016].

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing, 19(1), pp. 27-41

Wagner DeCew, J. (1986). The scope of privacy in law and ethics. Law and Philosophy, 5(2), 145-173.

Chiper Cloud, (2015). "Global guide to data protection".Internet: http://pages.ciphercloud.com/global-guide-to-data-protection-laws-landing-page.html, Nov. 20, 2015 [Oct. 02, 2016].

Hoven, J. V. D., Blaauw M., Pieters W.& Warnier M. "Privacy and Information Technology." Internet: http://plato.stanford.edu/entries/it-privacy/ , Nov. 20, 2014 [Nov.. 02, 2019].

Privacy International, (2016). "The Global Surveillance Industry". Internet: https://privacyinternational.org/explainer/1632/global-surveillance-industry, [Nov. 02, 2019].

Allison, S. F., Schuck, A. M., & Lersch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. Journal of Criminal Justice, 33(1), 19-29.

O'Brien, S (2019). "The Difference Between Data Privacy and Data Security". Internet: https://blog.cygilant.com/blog/the-difference-between-data-privacy-and-data-security, Oct. 22, 2019 [Nov. 2 , 2019]

CBSnews (2019) https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/ [July 31, 2019]

International Telecommunication Union (2006) "Research on legislation in data privacy, security and the prevention of cybercrime" Place des Nations CH-1211 Geneva, Switzerland (p. 69)

Keser, L., Kaya, M. B., & Kınıkoğlu, B. (2014). Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi. [Legal and Economic Analysis of the Personal Data Protection in Turkey] https://www.tepav.org.tr/upload/files/1421853130-9.Turkiyede_Kisisel_Verilerin_Korunmasinin_Ekonomik_ve_Hukuki_Analizi.pdf [Nov. 2, 2019]

Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. Columbia Law Review, pp. 583-676.

Ersoy, E. (2007). Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması [Privacy, Individual Rights, Protection of Personal Data]. Akademik Bilişim Konferansı 2007.

Turan M. (2016). Kişisel Verilerin Korunması [Protection of Personal Data] Türkiye Kalkınma Bankası Yayını, vol. 80, pp. 2-3 April-June, 2016

Henkoğlu, T., & Yılmaz, B. (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları [European Union (EU) Information Security Policies]. Türk Kütüphaneciliği, 27(3), 451-471.

Dedeoğlu, G. (2004). Gözetleme, Mahremiyet ve İnsan Onuru [Surveillance, Privacy and Human Dignity]. TBD Bilişim, 89, 36.

KVKK (2016). Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi [Legal and Economic Analysis of the Protection of Personal Data in Turkey] Internet:http://www.resmigazete.gov.tr/, Apr. 07, 2016 [Oct. 08, 2016].

Çırakoğlu, M. (2016). Düzenleyici Ve Denetleyici Kurulların Denetlenme Şekillerinin İdari Vesayet Bakımından Değerlendirilmesi [Evaluation of the Ways of Inspection of Regulatory and Supervisory Boards in terms of Administrative Guardianship.]. Yıldırım Beyazıt Hukuk Dergisi, (2).

Strahilevitz, L. (2013). Toward a positive theory of privacy law. Harvard Law Review, 113(1).

Nissenbaum, H. (2014). Respect for Context as a Benchmark for Privacy Online: What it Is and Isn't. Cahier de prospective, 19.

Schwartz, P. M. (2004). Property, privacy, and personal data. Harvard Law Review, 2056-2128.

Walch, D. (2011). Family Educational Rights and Privacy Act. Harmony, 503, 594-6000.

Code, U. S. (1999). Gramm-Leach-Bliley Act. Gramm-Leach-Bliley Act/AHIMA, American Health Information Management Association.

Stokes, R. (1999). Fair Credit Reporting Act., internet: https://www.consumer.ftc.gov/articles/pdf-0111-fair-credit-reporting-act.pdf [Nov. 2, 2019]

Onur, A (2013). Impact of Telecominications Regulation on Data Protection. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknolojileri Hukuku.

Privacy Act, (1974)." Privacy Act of 1974". Internet: https://foia.state.gov/Learn/PrivacyAct.aspx, Sep. 9, 2000 [Oct. 16 , 2016]

Küzeci, E. (2010). Kişisel Verilerin Korunması [Protection of Personal Data]. Turhan Kitabevi.

Kılınç, D. (2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması [Protection of Personal Data as a Constitutional Right], Anakara Üniversitesi Hukuk Fakültesi Dergisi, 61 (3) 2012:1089-1169

İzgi, M. C. (2014). Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri [Personal Health Data in the Context of the Privacy Concept]. Türkiye Biyoetik Dergisi, 1(1).

Karaarslan, E., Koç, S., & Akın, G. (2010). Vatandaşlık Numarası Bazlı E-Devlet Sistemlerinde Kişisel Veri Mahremiyeti Durum Saptaması [Personal Data Privacy Status Determination in Citizenship Number Based E-Government Systems] İzmir Bilişim Hukuk Kurultayı, 1-8.

Kaya, C. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi [Sensitive (Personal) Data and Processing on the Axis of the European Union Data Protection Directive]. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,vol. 69(1-2), 317-334.

Ketizmen, M., & Ülküderner, M. (2007). E-devlet uygulamalarında kişisel verilerin korun(ma)ması [protection (failure) of personal data in e-government applications]. XII."Türkiye'de İnternet" Konferansı.

Ceran A. (2014). Kişisel Verilerin Korunması: Avrupa ve Türkiye [Personal Data Protection: Europe and Turkey]. Iktisadi Kalkınma Vakfı Değerlendirme Notu, vol.104.

Karimi, O. & Korkmaz, A. (2013). Kişisel Verilerin Korunmasi [Personal Data Protection]. 18. Türkiye'de İnternet Konferansı inet-tr'13, İstanbul Üniversitesi, 9-11 Aralık 2013, İstanbul, Türkiye.

OECD (2008). OECD Policy Guidance on Online Identity Theft, Internet: http://www.oecd.org/sti/consumer/40879136.pdf , [Nov. 2, 2019]

ISO/IEC 29134 (2017), ISO/IEC 29134:2017**,** Guidelines for privacy impact assessment, internet: https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-1:v1:en

ICO (2015). Conducting privacy impact assessments code of practice. Internet: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf [Oct. 02 , 2019]

SEC (2007). Privacy Impact Assessment (PIA) Guide. Privacy Office of Information Technology. Internet: https://www.sec.gov/about/privacy/piaguide.pdf [Nov. 2, 2019]

IPC (2015). " Information and Privacy Commissioner of Ontario: ", Planning-for-Success Privacy Impact Assessment Guide, Internet: https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf [02 Nov. 2019]

HIQA (2017). Guidance on Privacy Impact Assessment in health and social care, Health Information and Quality Authority, Internet: https://www.hiqa.ie/sites/default/files/2017-10/Guidance-on-Privacy-Impact-Assessment-in-health-and-social-care.pdf, Oct. 2017 [Nov. 02 , 2019]

GDPR (2016). Regulatıon (Eu) 2016/679 Of The European Parliament And Of The Council Act. Official Journal Of European Union, (65).

CSX (2015). " Cyber Security Nexus Cyber Security Fundamentals". Internet: https://www.isaca.org/cyber, Jan. 1, 2015 [Oct. 28 , 2016], pp 77-82.

New York Times (2018), https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html, *New York Times*, Dec. 11, 2018, [july 31 2019]

Pascual A., Marchini K. & Miller S. "2016 Identity Fraud: Fraud Hits an Inflection Point." Internet:www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point , Feb. 02, 2016 [Oct. 02, 2016].

Lindén, F. (2009). epsos, smart open services for European patients from strategies to services health as the enabler for cross-border healthcare. *Infrastructures for Health Care*, *23*.

Dülger, M.V. (2019a). Kişisel Verilerin Korunması Hukuku [Personal Data Protection Law]. İstanbul: Hukuk Akademisi Yayıncılık

Dülger, M. V. (2019b). First Major Breach of the GDPR: France Fined Google€ 50.000. 000. *Available at SSRN 3331321*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331321

Dülger, M. V. (2018) İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması [Protection of Personal Data in the Context of Human Rights and Fundamental Rights and Freedoms]. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 5 (1), Bahar 2018

Kayyali, B., Knott, D., & van Kuiken S. (2013), The 'big data' revolution in healthcare: Accelerating value and innovation, McKinsey Global Institute Report, https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-big-data-revolution-in-us-health-care [Nov. 02, 2019].

Wang, Y., Kung, L., & Byrd, T. A. (2018). Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technological Forecasting and Social Change*, *126*, 3-13.

Yu, K. H., Beam, A. L., & Kohane, I. S. (2018). Artificial intelligence in healthcare. *Nature biomedical engineering*, *2*(10), 719-731.

Pendley, J. A. (2018). Finance and Accounting Professionals and Cybersecurity Awareness. *Journal of Corporate Accounting & Finance*, *29*(1), 53-58.

Aggarwal, A. K. (2019). Opportunities and challenges of big data in public sector. In *Web Services: Concepts, Methodologies, Tools, and Applications* (pp. 1749-1761). IGI Global.