DOI: https://doi.org/10.36719/2663-4619/87/29-33

Sama Arif Ahmadova
Baku State University
master student
ehmedovasema2022@gmail.com

LEGAL REGIME OF PERSONAL DATA COLLECTION AND EXISTING PROBLEMS

Abstract

Personal data can be any information that allows the identification of a person, directly or indirectly. It also contains a collection of information about personal and family life. In the era of rapid development of information and communication technologies, protection of personal data has become one of the top priorities of states. In the article, the legal regime of personal data, as well as the problems that may arise during the collection of personal data are analyzed, and various court cases are examined with reference to international and local legislation.

Keywords: *personal data, sensitive information, collection of personal information, data breaches, legal liability, data protection*

Səma Arif qızı Əhmədova
Bakı Dövlət Universiteti
magistrant
ehmedovasema2022@gmail.com

Fərdi məlumatların toplanmasının hüquqi rejimi və mövcud problemlər

Xülasə

Fərdi məlumatlara şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumatı aid etmək olar. Bu, həmçinin şəxsi və ailə həyatına dair məlumatların məcmusunu da ehtiva edir. İnformasiya və kommunikasiya texnologiyalarının sürətlə inkişaf etdiyi dövrdə fərdi məlumatların qorunması dövlətlərin prioritet məsələlərindən birinə çevrilib. Məqalədə fərdi məlumatların hüquqi rejimi, eyni zamanda fərdi məlumatların toplanılması zamanı ortaya çıxa biləcək problemlər təhlil olunmuş, beynəlxalq və yerli qanunvericiliyə istinad olunaraq müxtəlif məhkəmə işləri araşdırılmışdır.

Açar sözlər: *fərdi məlumatlar, fərdi məlumatların toplanması, pozuntular, hüquqi məsuliyyət, fərdi məlumatların mühafizəsi*

Introduction

Personal data refers to information that identifies or can be used to identify a specific individual. This can include names, addresses, phone numbers, email addresses, and other personal information. According to the Law of the Republic of Azerbaijan "On Personal Data," this type of data is defined as "any information that allows to directly or indirectly determine the identity of a person" (2). According to the Law of the Republic of Azerbaijan "On Obtaining Information," "personal information is a set of information about personal and family life." The range of personal information that is restricted is also specified by this regulation (3). Personal data can also encompass less traditional forms of identification, such as online identifiers, IP addresses, or device IDs. Personal data protection is regarded as a fundamental right in many countries, with numerous laws and regulations in place to ensure its privacy and security (5).

I. Legal regime of collection of personal data.

In today's digital age, various organizations, including governments, corporations, and other entities, collect and store massive amounts of personal data. The collection and storage of personal

data refers to the process of gathering, accumulating, and retaining information about individuals, usually through digital means. Personal data can be collected through various sources, such as online forms, social media, cookies, mobile applications, etc., and stored in various forms, such as databases, cloud storage, or physical storage mediums like hard drives or servers. This process must be in compliance with data protection laws and regulations, which set rules and standards for the handling of personal data. These laws often require organizations to implement appropriate technical and organizational measures to ensure the security of personal data and respect individuals' rights over their personal data. The purpose of collecting and storing personal data must be specified and limited to what is necessary for a legitimate purpose, and individuals must give their consent for their data to be collected and used. Otherwise, the widespread use of personal data may lead to concerns about privacy, security, and how it will be used. Numerous court cases have dealt with this in practice; one of these is Marper v. the United Kingdom, which might be noted. The misuse of personal information by an enterprise was the issue in this case, which was raised before the European Court of Human Rights (ECHR). The issue included the police's storage of DNA profiles and samples from people who had been detained but had not been found guilty of a crime. According to the ECHR, the storage of this personal data violated Article 8 of the European Convention on Human Rights, which guarantees the right to respect for one's private life. The court determined that the retention of this personal data was unreasonable and failed to strike a fair balance between the interests of the individual and the state because it was blanket and indiscriminate in nature. The ECHR came to the conclusion that the individual's right to privacy had been breached and that the storage of personal data was unnecessary in a democratic society (8). The case demonstrates that the collecting, processing, and storage of personal data must be done in line with legal requirements and must not interfere with the rights and liberties of others.

The collection of personal data by government agencies has become one of the main topics of discussion in recent years. On the one hand, governments argue that the collection of personal information is necessary for national security, law enforcement, and other public safety reasons. It can be used to prevent crime and protect public safety. In order to ensure national security as well as the rule of law, the legislation of the Republic of Azerbaijan defines the rules regarding the collection and processing of personal data related to the implementation of intelligence and counterintelligence, operational search activities, and the protection of personal data related to state secrets and collected in the national archive fund (2). On the other hand, privacy advocates argue that such data collection can be misused and lead to violations of individual rights and freedoms. This claim stems from the guarantee of the right to privacy (Article 32 of the Constitution of the Republic of Azerbaijan), because everyone has the right to keep the secrets of their personal and family lives (1).

II. Collection of personal data for commercial purposes.

One of the main reasons personal data is collected is for commercial purposes. Companies want to know as much about their customers as possible in order to target their marketing and advertising efforts more effectively. They use this information to create detailed profiles of individual consumers and their behaviors. This allows them to personalize their offerings, making them more appealing and increasing the likelihood of a sale. Companies collect personal data for various purposes, including:

- Customer relationship management: To improve customer relationships and experiences, companies collect personal data such as contact information, preferences, and purchase history.
- Fraud detection and prevention: To prevent fraud, companies collect and store personal data to detect and prevent suspicious activity.
- Product development: Companies use personal data to develop new products and services that are more appealing to consumers.
- Risk management: Companies use personal data to manage risk, such as by identifying potential credit risks or preventing money laundering.

- Compliance with legal requirements: Companies may be required by law to collect and store personal data for regulatory or legal purposes (13).

Overall, the collection of personal data allows companies to gain insights into consumer behavior, personalize their offerings, and make informed business decisions. Additionally, there are dangers associated with using personal data for commercial purposes. One of the key concerns is the potential misuse or abuse of personal data. If a company's database is compromised, for instance, sensitive data, such as social security numbers and bank account details, may be taken and used illegally. As a result, victims of data theft may experience identity theft, financial loss, and other problems. An example of this is the event that happened at Marriott International in 2018. Thus, the hotel faced a data breach that affected the personal information of millions of customers. Names, addresses, phone numbers, email addresses, passport numbers, dates of birth, gender, Starwood Preferred Guest account information, and encrypted payment card information were among the personal data exposed by the incident. The breach was discovered in November 2018, and the company determined that the breach had been ongoing since 2014. The company was heavily chastised for both the breach and its initial response, which included a delay in downplaying and warning (11). The incident has led to a number of lawsuits, including class-action lawsuits, as well as investigations by government agencies such as the Information Commissioner's Office (ICO) in the UK (10) and the Federal Trade Commission (FTC) in the US (9).

From a legal standpoint, the Marriott data breach emphasizes how important it is for businesses to take the necessary precautions to secure the personal information of their consumers. This includes putting in place the necessary organizational and technical safeguards to prevent violations, as well as responding to and notifying infractions as soon as they occur. Companies that fail to appropriately protect personal data may be subject to liability under data protection rules like the EU's General Data Protection Regulation (GDPR). In this case, several provisions of the GDPR may apply, in particular to matters of liability. Thus, Article 5(1)(f) of the GDPR requires appropriate personal data security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, through the use of appropriate technical or organizational methods.requires processing in such a way as to ensure Article 32 requires organizations to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including anonymization and encryption of personal data. In addition, the GDPR also defines administrative fines and the liability of processors that can be applied to organizations that violate these rules (7).

Marriott International may be held liable for failing to put in place the necessary security safeguards to safeguard personal data and guard against unauthorized access or misuse, as well as for failing to take preventative steps to lessen the effects of a data breach. A person's reputation and general well-being may suffer as a result of the misuse of personal information, which can also result in privacy violations and a loss of control over personal information. Since businesses use the data to judge people's creditworthiness and other factors that might have a big impact on their lives, the acquisition of personal data may also lead to discrimination.

III. Sharing personal information with third parties.

Another issue is the potential for the sharing of personal data with third parties without the person's knowledge or consent. This may occur when businesses rent or sell their client lists to other businesses. Due to the major privacy issues it creates and the possibility that some people may not want their personal information shared with others, this practice is contentious. In accordance with the Law of the Republic of Azerbaijan "On Personal Data", confidential personal data is protected by the leveler, operator, and appendices, who have the right of access to this data in accordance with the requirements stipulated in the legislation. Confidential personal data may be provided to third parties only with the consent of the subject, except in cases established by law (2).

Without the person's knowledge or consent, personal information may be disclosed to third parties, which may violate their right to privacy and expose them to possible misuse (Əliyev,

Rzayeva, İbrahimova, Məhərrəmov, Məmmədrzalı, 2019: 217). Lack of privacy control can lead to unauthorized marketing, identity theft, financial fraud, and other privacy violations. People should take precautions to preserve their personal information and be aware of what information is collected about them, how it is shared, and with whom it is shared. Companies must comply with GDPR by having privacy policies in place that clearly outline their data protection procedures and the rights of individuals with regard to their personal data. They are also responsible for ensuring that their systems and processes are secure, and that any third parties they share data with are also compliant with GDPR. This includes conducting risk assessments, implementing appropriate technical and organizational measures, and reporting data breaches to relevant authorities within 72 hours of becoming aware of them. Companies must also appoint a data protection officer if necessary and provide appropriate training to their employees on General Data Protection Regulation (GDPR) compliance (7).

One notable case is the Cambridge Analytica scandal, in which millions of Facebook users' personal information was gathered without their knowledge and exploited for political advertising. The Cambridge Analytica scandal involved the illegal collection of personal information from millions of Facebook users by political consulting firm Cambridge Analytica in the early months of 2018. Facebook was accused of giving Cambridge Analytica, a political consulting firm, improper access to the personal information of millions of Facebook users. Later, this private data was employed to affect the results of political contests, including the 2016 US presidential election (12). The legal aspect of the incident focuses on whether Facebook and Cambridge Analytica broke any privacy or data protection laws. This includes potential contraventions of national data protection laws, such as the Computer Fraud and Abuse Act of 1984 in the United States (6) and the General Data Protection Regulation (GDPR) in the European Union (7).

From a legal perspective, the question of liability in the Facebook and Cambridge Analytica scandal revolves around the question of whether Facebook failed to adequately protect the personal data of its users and who, if any, should be held responsible for that failure. While some contend that Facebook should be held responsible for the improper use of personal information by third parties like Cambridge Analytica, others contend that people should be held responsible for their own online security and data protection. The scandal sparked debate about the need for stronger privacy rules and led to numerous lawsuits against Facebook. The UK Information Commissioner's Office fined Cambridge Analytica and Facebook for breaching data protection laws, including failing to obtain valid consent for the collection and use of personal data. This case highlights the importance of ensuring that personal data is collected and used in accordance with relevant laws and regulations, with the informed consent of the relevant individuals.

Conclusion

Many countries have enacted laws and regulations to protect personal information. For example, the General Data Protection Regulation (GDPR) in the European Union provides specific guidelines for the collection of personal data by public authorities. The GDPR requires that such collection be limited to what is necessary and proportionate to the purpose of the collection. It also requires that individuals be informed of the collection of their data and be given the right to access and control their data.

In conclusion, let's note that personal data is a valuable commodity in the modern world, but it also causes great concern. The widespread collection and use of personal information has raised serious privacy and security issues, and it is important that individuals are aware of these issues and take steps to protect their personal information. Governments and organizations are also responsible for ensuring that personal information is collected, used, and stored responsibly and ethically. However, while the collection of personal data by government agencies may be necessary in some cases, it is also important to strike a balance between national security and privacy rights. This can be achieved by enforcing strict regulations and laws, as well as using secure systems and technologies to protect the data collected.

References

1. "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu. (2022). 11 may 2010-cu ildə qəbul edilmişdir (23 dekabr 2023-cü il tarixdə olan dəyişiklik və əlavələrlə). Bakı: "Azərbaycan" qəzeti, 31 dekabr.
2. "İnformasiya əldə etmək haqqında" Azərbaycan Respublikasının Qanunu. (2022). 30 sentyabr 2005-ci ildə qəbul edilmişdir (8 iyul 2022-ci il tarixdə olan dəyişiklik və əlavələrlə). Bakı: "Azərbaycan" qəzeti, 20 avqust, № 177.
3. Charter of Fundamental Rights of The European Union. (2012). 2000-Official Journal of the European Communities, OJ C 326, 26.10.2012, p.391-407.
4. Marper v. the United Kingdom, Application no. 30562/04 (European Court of Human Rights, Dec. 4, 2008).
5. Azərbaycan Respublikasının Konstitusiyası. (2016). 12 noyabr 1995-ci ildə qəbul edilmişdir (26 sentyabr 2016-cı il tarixdə olan dəyişiklik və əlavələrlə). Bakı: "Azərbaycan" qəzeti, 12 oktyabr, 224.
6. Max Freedman. (2023, January 23). How Businesses Are Collecting Data (And What They're Doing With It). Business News Daily. https://www.businessnewsdaily.com/10625-businesses-collecting-data.html
7. Marriott. (2018, November 30). Marriott announces Starwood guest reservation database security incident. Marriott News Center. https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident
8. ICO. (2019, July 9). Statement of Intent to fine Marriott International, Inc. more than £99 million. European Data Protection Board. https://edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-marriott-international-inc-more-ps99-million_en
9. Federal Trade Commission. (2018, December 3). Marriott Data Breach. Retrieved from https://www.consumer.ftc.gov/consumer-alerts/2018/12/marriott-data-breach
10. General Data Protection Regulation. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Official Journal of the European Union, L 119/1.
11. Əliyev, Ə., Rzayeva, G., İbrahimova, A., Məhərrəmov, B., Məmmədrzalı, Ş. (2019). İnformasiya hüququ. Dərslik. Bakı: "Nurlar" nəşriyyatı, 448 s.
12. Confessore, N., Hakim, D., & Keller, M.R. (2018, April 4). How Trump Consultants Exploited the Facebook Data of Millions. The New York Times. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
13. United States. Congress House. Committee on the Judiciary. (1984). Computer Fraud and Abuse Act of 1984. Washington, D.C.: U.S. Government Printing Office.

Reviewer: dr. of philosophy in law Bahruz Maharramov

Received: 13.11.2022 Accepted: 12.01.2023