DOI: https://doi.org/10.36719/2663-4619/88/46-51

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

THE ETHICS OF PERSONAL DATA COLLECTION AND USE

Abstract

In the digital age, personal information is collected and used in a variety of ways. With the growth of social media, the rise of e-commerce users, and the expansion of the use of Internet of Things (IoT) technology, more personal data is being stored and shared online. Although this data is quite necessary and important for businesses and organizations, it raises ethical concerns about confidentiality, consent and transparency when processing personal data. In this article, the current practice is analyzed based on international and local legislation, the ethics of collecting and using personal data is examined, and the impact of this trend on individuals and society as a whole is considered.

Keywords: *personal data, collection of personal information, data protection, use of personal information, ethics, privacy, consent, transparency*

Səma Əhmədova
Bakı Dövlət Universiteti
magistrant
ehmedovasema2022@gmail.com

Fərdi məlumatların toplanması və istifadəsi etikası

Xülasə

Rəqəmsal əsrdə fərdi məlumatlar müxtəlif yollarla toplanır və istifadə olunur. Sosial medianın inkişafı, elektron ticarətin istifadəçilərinin artması və Əşyaların İnterneti (IoT) texnologiyasından istifadənin genişlənməsi ilə fərdi məlumatlar daha çox onlayn olaraq saxlanılır və paylaşılır. Bu məlumatlar biznes və təşkilatlar üçün kifayət qədər lazımlı və vacib olsa da, fərdi məlumatların işlənilməsi zamanı konfidensiallıq, razılıq və şəffaflıqla bağlı etik narahatlıqları artırır. Bu məqalədə beynəlxalq və yerli qanunvericilik əsasında mövcud praktika təhlil olunaraq fərdi məlumatların toplanması və istifadəsi etikası araşdırılmış, bu tendensiyanın fərdlərə və bütövlükdə cəmiyyətə təsiri nəzərdən keçirilmişdir.

Açar sözlər: *fərdi məlumatlar, fərdi məlumatların toplanması, fərdi məlumatların mühafizəsi, fərdi məlumatların istifadəsi, etika, məxfilik, razılıq, şəffaflıq*

Introduction

Recent years have seen a significant increase in the collection of personal data by governments, businesses, and other organizations. This trend is driven by a number of factors, including the rise of digital technologies, the growing importance of data-driven decision-making, and the growing demand for personalized services and experiences. Also, with the development of social media, e-commerce, and the Internet of Things (IoT), more and more personal information is stored and shared online. Before we get into the ethics of collecting and using personal data, let's define what we mean by personal data. Personal data is any information that relates to an identified or identifiable living individual (7). This can include things like a person's name, address, date of birth, social security number, email address, phone number, and even IP address. It may also contain more sensitive information, such as a person's health records, financial information, and browsing history.

The collection and use of personal information can help businesses improve their marketing efforts, increase sales, and improve the customer experience. For individuals, personal information can provide access to personalized services and recommendations and help facilitate everyday tasks such as online shopping or banking (9). Despite the benefits of collecting and using personal data, there are also significant risks and concerns. One of the biggest risks is that personal data can be used for nefarious purposes such as identity theft, fraud, or cyberattacks. It can also be sold or shared without the individual's knowledge or consent, leading to a loss of privacy and control over personal information (8). Given the risks and concerns we have listed, it is important to consider the ethical implications of this trend. This highlights the importance of the ethics of collecting and using personal data and the need to study the impact of this trend on individuals and society as a whole.

Importance of Informed Consent in Personal Data Collection and Use - Informed consent is a crucial ethical factor to take into account while collecting and using personal data. Before collecting and processing personal data, businesses must get informed consent from people in many countries, according to laws and regulations. The General Data Protection Regulation (GDPR), a rule of the European Union that controls the gathering and processing of personal data, is one famous instance. Before collecting and using an individual's personal data, businesses must seek that person's express and specific consent under GDPR (7). By giving their consent, people may be sure that they are fully informed about how their data will be used and can decide for themselves whether or not to disclose it.

According to Article 8 of the Law of the Republic of Azerbaijan "On Personal Information", the collection and processing of personal information about any person is allowed only on the basis of written consent given by the subject. Written consent means consent in the form of an electronic document with an enhanced electronic signature or information provided in writing by oneself (1). In order to obtain consent, it is essential to inform people in a clear and simple manner about the reason for data collection, the legal basis for processing, and the duration of data retention. No matter their degree of technical expertise or education, everyone should be able to understand this information if it is presented in an approachable way. When collecting sensitive personal data, such as that pertaining to a person's health, ethnicity, religion, or sexual orientation, informed consent is especially crucial (10). People in these situations must expressly consent to the collection and processing of their data after being fully informed about how it will be used.

A key component of legislation and regulations governing data privacy is informed consent. Entities that fail to obtain individuals' informed consent may be subject to fines and other legal repercussions, including legal culpability. To guarantee that personal data is acquired and utilized in a legal and ethical manner, it is crucial that businesses prioritize informed consent as a core part of their data privacy practices. The 2017 Equifax data breach is yet another illustration of the significance of informed consent in the acquisition and use of personal information. Equifax, one of the largest credit reporting companies in the United States, suffered a major data breach in 2017 that compromised the personal information of more than 143 million people (6). Names, birthdates, Social Security numbers, addresses, and, in certain cases, driver's license numbers were among the data stolen. A breach in Equifax's website software led to the breach, which gave hackers access to the personal data of millions of people. Equifax obtained personal information without the clear and express consent of the interested parties. Those whose personal information was taken lacked control over it as well as a way to reject Equifax's data acquisition methods (12). The incident made clear the necessity for stricter laws governing data privacy. Equifax updated its data privacy policies in reaction to the incident and modified its data gathering procedures to make sure users are fully informed of how their data is being handled.

In conclusion, incidents like this serve as yet another reminder of the significance of ethical issues in the gathering and use of personal information. This emphasizes the significance of gaining individuals' informed consent and guaranteeing control over their personal information. To maintain

ethical data privacy policies and responsible and open gathering and use of personal information, organizations should emphasize these procedures.

Transparency in Personal Data Collection and Processing: An Ethical Imperative - As an ethical requirement, transparency in the gathering and processing of personal data has become more commonly recognized. Everyone has a right to information about the data that is gathered about them, how it is used, and who gets to see it. Companies gain customers' trust and show their dedication to proper data management when they are open and honest about how they gather and use client data. Individuals must be given clear and explicit information about how their data is gathered, processed, and used in order for data collection and processing to be transparent. The owner or operator shall expressly identify the purpose for collecting and using personal data, as required by Article 9.1 of the Law of the Republic of Azerbaijan on "Protection of Personal Data" (1).

In addition to doing this, information must be provided regarding the categories of data gathered, the uses to which the data is put, and the names of any third parties with whom the data is shared. Also, entities must give people clear explanations of their terms of service and privacy policies.

Transparency in data collection and processing is an ethical imperative because it helps users make informed decisions about their personal information. Individuals are better able to exercise their rights to access, modify, and delete their data when they are fully informed about how their data is being used.

Transparency also encourages accountability for companies that manage personal data and helps avoid the misuse of that data. Otherwise, privacy issues and data breaches can occur. An example is the Cambridge Analytica scandal, which involved the unauthorized collection and use of Facebook user data to influence political campaigns (5). The controversy emphasized the need for more openness in data gathering and processing procedures and increased public awareness of the significance of data privacy.

In conclusion, transparency in the gathering and use of personal data is a legal necessity that encourages accountability, motivates people, and develops trust. Companies that place a substantial priority on transparency in their data management procedures show their dedication to ethical data management and forge closer connections with customers.

Security and Confidentiality of Personal Data: Ethical Considerations for Organizations - The security and privacy of personal data are important issues for organizations that collect and process such data. Organizations are ethically obligated to maintain the security and confidentiality of the data they gather, in addition to the legal responsibilities for doing so. Therefore, it is necessary to look into the ethical issues surrounding the security and privacy of personal data. The Republic of Azerbaijan's Cabinet of Ministers determined that when processing personal data in information systems, fundamental organizational and technological security standards must be followed (2).

Ethical considerations for the security of personal data − Entities have a responsibility to make sure that personal data is secured from theft, loss, and unauthorized access. It is ethically required to preserve people's privacy and to take precautions against any potential harm that might result from unauthorized access to personal information. Basic technical and organizational safety requirements must be met in order to protect the security of personal data held by organizations, including the timely detection and prevention of facts indicating illegal interference, the possibility of immediately recovering changed or destroyed personal data, constant monitoring of the level of protection, the use of licensed software, the maintenance of an appropriate accounting system, etc. (2).

Ethical considerations regarding privacy of personal information − Secondly, organizations have a responsibility to guarantee that confidential data is protected and that only people with permission can access it. This commitment results from a moral duty to protect people's privacy and avoid potential harm from illegal access to personal information. Companies must set up the

necessary rules and procedures to guarantee that only authorized individuals can access personal information and that it is only used for the purposes for which it was gathered (7).

In general, the procedures to be followed to maintain the security and privacy of personal data can be separated into three stages:

- Data discovery: Companies need to learn what data sets exist in their systems, determine which are business vital, and determine which contain sensitive data subject to compliance rules.
- Deployment of numerous methods for data protection, including data loss prevention, internal data protection for storage, backups, snapshots, replication, firewalls, authentication and authorization, encryption, endpoint security, data deletion, and disaster recovery.
- Adherence to relevant legislation, such as GDPR, which may call for the deletion of superfluous data to reduce liability, must be ensured by organizations (4).

In practice, there are numerous cases related to violations of the security and privacy of personal data, one of which is the case of Szabo and Vissi v. Hungary, brought before the European Court of Human Rights (ECtHR).

The applicants in this case were two journalists investigating the use of surveillance technologies by the Hungarian government.

They discovered evidence that the government was using a powerful spyware program called Pegasus and published an article about it, but soon after, their own phones were infected with the same spyware. As a result of their investigations and reports, the journalists applied to the court, believing that their phones were infected with a virus and that their privacy and freedom of expression were violated. The ECtHR considered the Hungarian government's access to the personal data of the applicants through the use of spyware as an interference with the right to respect for private life (11).

This case demonstrates the importance of personal data security and privacy, especially in the context of government surveillance. The ECtHR decision recognized the importance of protecting the privacy of individuals, including journalists and human rights defenders, and confirmed the need for strong legal protection of personal data to protect individual rights and freedoms.

Accountability and Penalties for Non-Compliance: Ensuring Ethical Use of Personal Data

− In recent years, there has been increasing attention to the importance of liability and penalties for non-compliance with data protection regulations to ensure the ethical use of personal data. Organizations that collect and process personal data must be held accountable for their actions and penalized if they fail to comply with relevant laws and regulations.

One of the main examples of this is the European Union's General Data Protection Regulation (GDPR), which includes the obligation to provide transparent information about data processing activities and the requirement to implement appropriate security measures to protect personal data. Organizations that violate these responsibilities may be subject to severe penalties under the GDPR, including fines of up to 4% of their annual global revenue or €20 million, whichever is higher. These fines are meant to discourage non-compliance and motivate enterprises to take their GDPR commitments seriously (7). A fine between three hundred and five hundred manats is imposed for violating the law, according to Article 375 of the Republic of Azerbaijan's Code of Administrative Offenses (3).

The above-mentioned Facebook and Cambridge Analytica cases represent an important illustration of the significance of accountability and the imposition of sanctions for non-compliance. As a response to Facebook's failure to protect user data, the US Federal Trade Commission fined the company $5 billion (5).

This case demonstrates the value of holding companies accountable for their activities and the necessity of stiff sanctions for violations of data protection laws. By imposing sanctions on companies that break these rules, governments and authorities can assure the moral and responsible gathering and processing of personal data while protecting individuals' rights.

Conclusion

The investigation of ethical considerations related to the collection and use of personal data, the research conducted to determine the range of problems in this field, including the analysis of international and local legislation in this regard, have created the conditions for obtaining the following results.

- When processing personal data, organizations should have clearly stated policies and processes for the gathering and use of personal data. These policies and procedures should be made public and updated frequently as new regulations are introduced.
- Security measures should be improved, ensuring secure data gathering and storage with the use of firewalls and proper encryption.
- Before collecting and using a person's personal information, entities must have that person's explicit consent. This consent must be freely granted, relevant to the data's intended use, and informed.
- Governments should keep on making and implementing better privacy regulations that safeguard people from unethical uses of their personal information and promote a culture of ethical data use.

References

1. 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.
2. 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
3. GLS Law. (2021, November 24). What are the risks associated with collecting personal data? https://www.gls-startuplaw.com/blog/entry/what-are-the-risks-associated-with-collecting-personal-data
4. "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu. (2022). 11 may 2010-cu ildə qəbul edilmişdir (23 dekabr 2022-ci il tarixdə olan dəyişiklik və əlavələrlə). Bakı: "Azərbaycan" qəzeti, 31 dekabr.
5. Office of the Privacy Commissioner of Canada. (2018). Guidelines for Obtaining Meaningful Consent. https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/
6. Federal Trade Commission. (2019, July 22). Equifax data breach settlement. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement
7. United States Government Accountability Office. (2018). Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach. https://www.gao.gov/products/gao-18-559
8. 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
9. "Fərdi məlumatların mühafizəsinə dair Tələblər"in təsdiq edilməsi haqqında Azərbaycan Respublikası Nazirlər Kabinetinin Qərarı. (2022). 6 sentyabr 2010-cu ildə qəbul edilmişdir (25 avqust 2022-ci il tarixdə olan dəyişiklik və əlavələrlə). Bakı: "Xalq" qəzeti, 2 sentyabr.
10. Cloudian. (2021). Data protection and privacy: 7 ways to protect user data. https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/
11. Szabo and Vissi v. Hungary, Application nos. 37138/14 and 988/15, (European Court of Human Rights. Jan. 12, 2016).

12. Azərbaycan Respublikasının İnzibati Xətalar Məcəlləsi (2023). 29 dekabr 2015-ci ildə qəbul edilmişdir (30 dekabr 2022-ci il tarixdə olan dəyişiklik və əlavələrlə). Bakı: "Azərbaycan" qəzeti, 1 fevral, № 22.

Reviewer: dr. of philosophy in law Bahruz Maharramov

Received: 25.01.2023 Accepted: 27.02.2023