sciendo

Research Article

Human rights in the technology era – Protection of data rights

Vlona Pollozhani Shehu
Assistant Professor, University of Tetova

Visar Shehu
Associate Professor, South East European University

DOI: https://doi.org/10.2478/ejels-2023-0001

Abstract

Current advances in technology without any doubt bring numerous advancements to mankind, but also introduce new challenges in regard to human rights. This is particularly true in the context of data protection. Clearly, in the current digital age, data has great value. However, there are great concerns in regard to data collection, processing and its use. These concerns are related to privacy, transparency and accountability. In the technology era, the protection of data rights is crucial for upholding human rights in a digital society, as the widespread collection, storage, and use of personal data pose significant challenges to privacy, autonomy, and non-discrimination. This paper explores the intersection of human rights and data rights, analyzes the legal and ethical dimensions of data protection, and proposes strategies to ensure the effective safeguarding of data rights in order to uphold fundamental human rights principles in the digital age.

Keywords: human rights, data protection, data ownership.

1. Introduction

The rapid advancement of technology in recent decades has revolutionized the way we live, communicate, and interact with the world. From the internet and social media to artificial intelligence and big data, technology has become an integral part of our daily lives, shaping various aspects of society and raising important questions about human rights in the digital age. As our lives become increasingly interconnected through digital platforms and our personal information is stored and shared in unprecedented ways, the protection of data rights has emerged as a critical concern. Data rights refer to the rights individuals have over their personal data, including the

rights to privacy, control, and consent. In the technology era, where data is often described as the "new oil," the collection, storage, and use of personal data have become lucrative industries. However, this rapid growth in data-driven technologies has also brought about numerous challenges and risks. Issues such as data breaches, privacy infringements, surveillance practices, and algorithmic bias have raised fundamental questions about the extent to which individuals' data rights are respected and protected. To address these concerns and ensure the preservation of human rights in the technology era, it is crucial to explore the relationship between data rights and human rights, examine existing legal and ethical frameworks, and propose solutions for promoting and safeguarding data rights in a rapidly evolving technological landscape.

2. Understanding data rights

Data rights encompass the rights individuals have over their personal data, empowering them to exercise control, privacy, and consent in the digital realm. Understanding data rights is crucial in the technology era, where vast amounts of personal information are collected, stored, and utilized by various entities. These rights are closely tied to human rights, as the protection of data rights plays a vital role in preserving privacy, autonomy, and non-discrimination. By recognizing the value of personal data and the implications of its use, societies can navigate the complex ethical and legal landscape surrounding data rights.

Data rights consist of several key elements that empower individuals in the digital age. The right to privacy ensures that personal information remains confidential and protected from unauthorized access or use. Individuals also possess the right to control their data, allowing them to determine how their information is collected, stored, shared, and processed. Informed consent is another crucial aspect of data rights, requiring individuals to provide explicit and knowledgeable consent before their data is utilized. Furthermore, data rights encompass the right to access one's own data and the right to rectify or delete inaccuracies. These elements collectively form the foundation for empowering individuals and establishing a fair and transparent data ecosystem.

International legal frameworks and regulations play a significant role in the recognition and protection of data rights. The General Data Protection Regulation (GDPR) in the European Union, for instance, sets standards for data protection, establishing principles such as data minimization, purpose limitation, and accountability. Similarly, the California Consumer Privacy Act (CCPA) in the United States grants individuals certain rights over their personal data and imposes obligations on businesses. These legal frameworks aim to ensure that data processing activities are conducted responsibly, with individuals' rights and privacy rights in focus.

Despite the progress made in recognizing and safeguarding data rights, there are ongoing debates and challenges in this domain. One key area of discussion is the balance between individual rights and societal benefits derived from data utilization. The tension between privacy and innovation often requires careful consideration and

policy-making. Additionally, the rise of emerging technologies like artificial intelligence and machine learning introduces concerns regarding algorithmic bias and discrimination. As data-driven decision-making becomes more prevalent, addressing these challenges and maintaining robust data rights protections remains essential.
The connection between data rights and human rights lies in the preservation of privacy and autonomy. Privacy is a fundamental human right recognized by various international agreements and declarations. In the digital age, the protection of personal data is essential for safeguarding privacy. Data rights provide individuals with the ability to control the collection, use and disclosure of their personal information. This control empowers individuals to maintain their autonomy and make informed decisions about the dissemination of their data. Without robust data rights protections, individuals may be subject to unwanted surveillance, data breaches, or manipulative targeting, eroding their right to privacy and infringing upon their autonomy.
Data rights are also closely tied to the principle of non-discrimination and the promotion of fair treatment. In the technology era, data-driven decision-making processes can significantly impact individuals' opportunities and experiences. The collection and analysis of personal data can lead to the creation of profiles or algorithms that make decisions about individuals, such as employment opportunities, financial access, or resource allocation. If these processes are not governed by strong data rights protections, there is a risk of perpetuating biases and discrimination. Data rights, therefore, play a crucial role in ensuring that individuals are not unfairly treated or discriminated against based on their personal characteristics or attributes. By recognizing and protecting data rights, societies can strive for fair and equitable treatment, promoting equal opportunities and upholding the principles of human rights.

3. **Literature review**

A systematic literature review was conducted with a purpose of determining what similar research has been conducted and to compare the different mechanisms that protect data and privacy rights. The focus has been on the two major initiatives, the General Data Protection Regulation (GDPR)[1] and California Consumer Privacy Act (CCPA).[2]
According to Xiao (2019) personal data rights should be protected through a combination of private rights and tort law. On the other hand, Pintiliuc (2018) suggests that individuals have a fundamental right to privacy and intimate life that must be protected.
In a different approach, (Samuelson, 2000) argues that the notion of assigning personal information ownership rights to individuals may not necessarily fulfill the objectives of information privacy. This is partly due to a fundamental principle of property

[1] Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).
[2] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199 (West 2020).

law - the free transferability of rights, which could inadvertently compromise rather than support information privacy aims.

The EU has specific legislative acts and regulations in place to guarantee a high level of data protection for citizens, institutions, and partners (Coulson, 2009). Overall, the paper suggests that personal data rights should be protected through a combination of legal frameworks and regulations that balance the interests of individuals and data companies.

There are mechanisms in place that are addressing this issue. One of them is General Data Protection Regulation (GDPR) which is a regulatory framework introduced by the European Union in 2018 to protect the privacy and personal data of its citizens. It places stricter controls on businesses and organizations, compelling them to be transparent about how they collect, process, store, and use personal data. The GDPR also grants individuals greater control over their personal information, including the right to access their data, correct inaccuracies, object to processing, have their data deleted, and more. It applies to all companies operating within the EU, as well as to organizations outside the EU that offer goods or services to EU residents or monitor their behavior. Non-compliance can result in hefty fines, emphasizing the importance of data protection in today's digital world.

In the United States, there isn't a direct, federal equivalent to the EU's GDPR. U.S. privacy laws are a patchwork of federal and state regulations that each address different areas, sectors, or types of data. However, the California Consumer Privacy Act (CCPA), which came into effect in 2020, is the closest analogue. The CCPA gives California residents rights like those of the GDPR, including the right to know what personal information businesses collect about them, to delete that information, and to opt-out of the sale of that information. Despite this, the reach of the CCPA is limited to California, and there's ongoing debate about whether a more comprehensive federal data privacy law should be enacted.

The effectiveness of GDPR and CCPA has been also subject of research in the past. In general, a consensus is that GDPR is effective in protecting data privacy and imposing obligations on organizations regarding the storing, processing, collecting, and disclosing of data. Concerns are mostly related to the effect of GDPR to IT operations for different companies.

Bartolini (2019) argues that GDPR has brought significant changes to data protection laws in the European Union, prompting the need for solutions that help controllers and processors comply with these requirements. One proposed solution according to them is integrating privacy concepts into Business Process (BP) models, allowing for GDPR recommendations to be included in specific tasks of the BP, improving process management and personnel training.

Regarding the effect on the IT processes (Teixeira, 2019) identifies critical success factors for GDPR implementation, including barriers and enablers, and benefits of complying with GDPR.

Tsekoura (2020) provides a critical review of the practical, ethical, and constitutional aspects of GDPR one year after its implementation, highlighting the heightened awareness of data protection issues and the efforts of data controllers and processors

to achieve GDPR compliance.
Finally, Murphy (2018) argues that GDPR introduces significant changes to the IT operations of businesses and the way they process personal data of their EU resident customers, with a single set of rules applying to all EU member states and each member state establishing an independent Supervisory Authority to sanction administrative offenses and investigate complaints.
When comparing GDPR with CCPA, the effectiveness of each measure depends on the specific context and objectives. The GDPR provides more extensive protection and has a broader scope, affecting businesses that process personal data of EU citizens. It also carries more severe penalties. The CCPA, while limited to California, has been influential in driving privacy legislation discussions in the United States and has prompted other states to adopt similar laws.
Scholars comparing these two measures, suggest that while CCPA and GDPR have similarities, there are also substantial differences in their approaches to data protection and cross-border data transfers. Bukaty (2019) notes that CCPA is the strictest privacy legislation in the US and expands liability for consumer data breaches. Gallagher (2018) provides a comparison of the two regulations, highlighting similarities and differences. He concludes that CCPA is more effective than GDPR, although it is not a federal law in USA. Ooijen (2018) analyzes the extent to which GDPR enhances consumers' control over personal data and identifies the pitfalls of human decision-making that threaten individual control. Finally, Sullivan (2019) compares the approaches of the EU and APEC to cross-border data transfers and protection of personal data in the IoT era.

4. Notable examples of data rights violations

The following examples demonstrate the importance of robust data protection measures, ethical data handling practices, and regulatory oversight to prevent data rights violations. They serve as reminders of the need for individuals, organizations, and governments to prioritize the protection of personal data and uphold the rights of individuals in an increasingly data-driven world.
In 2018, it was revealed that the political consulting firm Cambridge Analytica obtained the personal data of millions of Facebook users without their explicit consent. The data was used for targeted political advertising during the U.S. presidential election in 2016. This incident highlighted the potential misuse and unauthorized access to personal data by third-party entities, leading to a global debate on data privacy and the need for stricter regulations.
In 2017, Equifax, one of the largest credit reporting agencies in the United States, suffered a massive data breach that exposed sensitive personal information, including Social Security numbers and credit card details, of approximately 147 million consumers. The breach not only highlighted the vulnerability of vast databases containing personal data but also raised concerns about the security practices and response mechanisms of organizations handling sensitive information.
In 2017, ride-hailing company Uber faced criticism for its handling of a data breach

that occurred in 2016. Instead of disclosing the breach to the affected users and relevant authorities promptly, Uber paid a ransom to the hackers to delete the stolen data and attempted to cover up the incident. This incident highlighted the importance of transparency, accountability, and timely disclosure of data breaches to protect users' rights and mitigate potential harm.

Aadhaar is India's biometric identification system, which collects and stores personal information of over a billion citizens. Several instances of data breaches and privacy concerns have emerged, including cases where Aadhaar details were leaked or sold on the black market. These incidents have raised questions about the security and integrity of such large-scale biometric databases and the potential risks associated with the misuse of personal data.

However, there are success stories as well.

Following the Cambridge Analytica scandal, Facebook faced widespread criticism for its handling of user data and privacy breaches. As a result, regulatory authorities and advocacy groups pushed for stronger data protection measures and transparency. In 2019, Facebook reached a settlement with the U.S. Federal Trade Commission (FTC) requiring the company to pay a record-breaking fine and implement stricter privacy controls. The settlement also mandated changes in Facebook's data practices to enhance user privacy, provide clearer consent mechanisms, and establish an independent privacy committee. This case highlighted the importance of holding tech giants accountable and advocating for stronger privacy protections.

In 2018, Microsoft challenged a U.S. government warrant seeking access to customer data stored in an overseas data center.[3] The case involved the question of whether U.S. law enforcement could compel a company to provide data stored outside the United States. In 2018, the U.S. Supreme Court ruled in favor of Microsoft, stating that U.S. warrants did not have extraterritorial reach. This case highlighted the importance of jurisdictional boundaries and the need to balance law enforcement interests with privacy and data protection rights.

Revelations by whistleblowers, such as Edward Snowden, about government surveillance programs like PRISM and Tempora sparked significant public outcry and debate. These revelations led to increased awareness about the extent of mass surveillance and its impact on privacy and civil liberties. The public backlash prompted discussions on the balance between security and privacy, leading to reforms, increased transparency, and more stringent oversight of government surveillance practices in various countries.

5. **Future directions and recommendations**

To strengthen legal frameworks for data rights, it is essential to enact comprehensive data protection laws that provide clear guidelines and regulations for the collection, storage, and use of personal data. These laws should encompass principles such as data minimization, purpose limitation, and informed consent. They should also include provisions for individuals to exercise their rights over their personal data, such

[3] United States v. Microsoft Corp., 138 S. Ct. 1186, 200 L. Ed. 2d 610 (2018).

as the right to access, rectify, and delete their information. Examples of effective data protection laws include the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which establish strong rights for individuals and impose obligations on organizations handling personal data. By implementing robust and harmonized data protection laws, governments can ensure consistent and comprehensive protection of data rights across sectors and jurisdictions.

Strengthening legal frameworks for data rights also requires enhanced enforcement mechanisms and penalties for non-compliance. It is crucial to establish independent regulatory authorities with the power to investigate data breaches, monitor data practices, and impose fines or sanctions for violations. Effective enforcement ensures that organizations take data protection seriously and encourages them to adopt privacy-by-design principles. Fines and penalties should be proportionate to the severity of the violation, taking into account factors such as the nature of the breach, the scale of the harm caused, and the financial resources of the organization. By implementing strong enforcement mechanisms and penalties, legal frameworks can act as effective deterrents and promote accountability in data handling practices.

Data flows do not respect national borders, and protecting data rights often requires international cooperation and harmonization of legal frameworks. Governments should work collaboratively with international organizations, such as the United Nations and the International Organization for Standardization (ISO), to develop common standards and principles for data protection. This cooperation can help bridge gaps in legislation, facilitate cross-border data transfers, and promote a global understanding of data rights. Additionally, bilateral and multilateral agreements can be established to ensure the protection of personal data when transferred between countries. By fostering international cooperation and harmonization, legal frameworks for data rights can address the challenges posed by the global nature of data and promote consistent and high standards of data protection worldwide.

Technological solutions are also crucial when addressing these issues. Some of them are as follows:

Advancing technological solutions for data privacy involves the widespread adoption of robust encryption techniques and data security measures. Encryption plays a critical role in protecting sensitive information by encoding it in a way that can only be accessed by authorized parties. Encrypted data is more resistant to unauthorized access and can mitigate the risks of data breaches. Moreover, technologies such as secure communication protocols and secure socket layers (SSL) can safeguard data during transmission. By promoting the development and implementation of strong encryption algorithms, governments and organizations can enhance data privacy and provide individuals with greater confidence in the security of their personal information.

One positive example we have researched in this regard is the LetsEncrypt initiative. In the past obtaining SSL certificates for web sites was a technically challenging and expensive endeavor. LetsEncrypt is a nonprofit Certificate Authority that enables citizens to obtain free SSL certificates to protect their web sites. In their annual report for

2022 (Internet Security Research Group, 2022), there have been 3,078,399,255 certificates issued since 2015 by this authority, with 239,710,300 active certificates.

With LetsEncrypt, there are no reasons for a web site to be unsecure and to allow for unencrypted user data transfers through unencrypted channels. We strongly believe that strong legal mechanisms should be put in place that will require for companies and individuals to implement SSL for every web site that collects or uses user data.

Another technological solution is to implement privacy-enhancing technologies (PETs). These technologies offer innovative solutions to protect individuals' data while still allowing for data processing and analysis. PETs include techniques such as differential privacy, federated learning, and homomorphic encryption. Differential privacy provides a framework to collect and aggregate data while preserving individuals' privacy by injecting noise into the data to protect identities. Federated learning enables collaborative model training without sharing raw data, ensuring privacy while leveraging collective intelligence. Homomorphic encryption allows computations on encrypted data, keeping sensitive information secure even during analysis. By encouraging research and development in PETs and promoting their adoption, data privacy can be enhanced without compromising the benefits derived from data-driven technologies.

Finally, it is important for IT companies to understand that their solutions need to implement privacy by design and to minimize collection of data to the absolute necessary minimum. Privacy by design emphasizes integrating privacy measures into the design and architecture of technological systems from the outset. By incorporating privacy features such as granular consent mechanisms, default privacy settings, and anonymization techniques, privacy by design ensures that data privacy is a fundamental consideration in every stage of system development. Furthermore, data minimization practices involve limiting the collection and retention of personal data to what is strictly necessary for the intended purpose. By reducing the amount of personal data collected and stored, the risk of data breaches and unauthorized access is mitigated. Emphasizing privacy by design and data minimization not only enhances data privacy but also promotes transparency, user control, and accountability in the digital ecosystem.

As we mentioned earlier, data flow does not respect borders. Promoting global cooperation and collaboration in data rights involves facilitating the sharing of best practices and knowledge exchange among countries, organizations, and stakeholders. By sharing successful strategies, lessons learned, and innovative approaches, countries can learn from one another and adopt effective measures to protect data rights. International forums, conferences, and working groups can serve as platforms for fostering dialogue and collaboration on data privacy issues. Through these exchanges, countries can develop a collective understanding of challenges and identify common goals, leading to the development of harmonized standards and guidelines that promote data rights and facilitate global collaboration in safeguarding personal information.

With the increasing globalization of data flows, cross-border data transfers have become a critical aspect of the digital economy. Promoting global cooperation involves

establishing cross-border data transfer agreements that strike a balance between privacy protection and the free flow of data. These agreements can provide a framework for countries to mutually recognize and trust each other's data protection laws, ensuring that personal data is adequately protected when transferred between jurisdictions. Examples of such agreements include the EU's adequacy decisions, which allow for data transfers to countries that are deemed to provide an adequate level of data protection. By promoting cross-border data transfer agreements, countries can facilitate international business operations while maintaining robust data privacy standards.

As data becomes an increasingly valuable resource, multilateral collaboration on data governance is crucial to address complex challenges and promote harmonization of standards. International organizations and initiatives can play a vital role in facilitating this collaboration. For instance, the United Nations (UN) and its agencies can serve as platforms for developing global principles and guidelines for data protection. Additionally, collaborative efforts such as the Global Privacy Assembly (formerly known as the International Conference of Data Protection and Privacy Commissioners) bring together privacy and data protection authorities from around the world to share experiences, exchange information, and coordinate on common issues. Through multilateral collaboration on data governance, countries can work together to establish norms, foster trust, and ensure that data rights are protected in a globally interconnected digital environment.

6. Conclusion

In conclusion, strengthening legal frameworks for data rights is crucial in the technology era to protect individuals' privacy, autonomy, and non-discrimination. Comprehensive data protection laws that encompass principles such as data minimization, purpose limitation, and informed consent are essential. These laws should provide individuals with rights to access, rectify, and delete their personal data, while independent regulatory authorities should be empowered to enforce compliance with these laws through penalties and fines. Additionally, international cooperation and harmonization of legal frameworks are necessary to address the global nature of data and establish common standards for data protection. Cross-border data transfer agreements and multilateral collaboration on data governance can promote trust, facilitate secure data flows, and ensure consistent high standards of data protection globally.

Technological solutions play a crucial role in advancing data privacy. Robust encryption techniques and data security measures, such as secure communication protocols and SSL, enhance the security of personal information. Privacy-enhancing technologies (PETs) like differential privacy, federated learning, and homomorphic encryption enable data processing while preserving privacy. Implementing privacy by design and data minimization practices ensures that privacy considerations are integrated into technological systems from the outset and reduces the collection and storage of unnecessary personal data. These technological solutions provide individuals with

greater confidence in the security of their data and enable responsible data practices. Promoting global cooperation and collaboration is paramount in safeguarding data rights. Sharing best practices and knowledge exchange among countries and organizations foster learning and adoption of effective measures. Cross-border data transfer agreements strike a balance between privacy protection and data flows, ensuring that personal data is adequately protected during international transfers. Multilateral collaboration on data governance through international organizations and initiatives establishes common principles and guidelines for data protection, fostering trust and consistency across jurisdictions.

In the pursuit of protecting data rights in the technology era, it is crucial for governments, organizations, and individuals to work collectively. Strengthening legal frameworks, advancing technological solutions, and promoting global cooperation are interdependent components of an effective strategy. By prioritizing data rights, we can ensure that the tremendous benefits of technology are accompanied by robust protections, empowering individuals, and fostering a digital environment that respects privacy, autonomy, and non-discrimination. It is only through these collective efforts that we can safeguard fundamental human rights in the ever-evolving landscape of technology.

References

Bartolini, C., Calabrò, A., & Marchetti, E. (2019). GDPR and business processes: an effective solution. Proceedings of the 2nd International Conference on Applications of Intelligent Systems.

Bukaty, P. (2019). The California Consumer Privacy Act (CCPA).

Coulson, A., & Payne, H. (2009). Data Protection. The Veterinary record, 147 20, 583.

Gallagher, B.J. (2018). A Comparison of GDPR and CCPA | I.S. Partners | Compliance Advisors.

Murphy, J.F. (2018). The General Data Protection Regulation (GDPR). Irish medical journal, 111 5, 747.

Pintiliuc, I. (2018). Protection of personal data. Logos Universality Mentality Education Novelty: Law.

Ooijen, I.V., & Vrabec, H.U. (2018). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. Journal of Consumer Policy, 42, 91-107.

Samuelson, P. (2000). Privacy as intellectual property.

Teixeira, G.A., Silva, M.M., & Pereira, R. (2019). The critical success factors of GDPR implementation: a systematic literature review. Digital Policy, Regulation and Governance.

Tsekoura, T.M., & Panagopoulou, F. (2020). GDPR: a critical review of the practical, ethical and constitutional aspects one year after it entered into force. International Journal of Human Rights and Constitutional Studies.

Xiao, C. (2019). Personal Data Rights in the Era of Big Data*. Social Sciences in China, 40, 174 - 188.

Internet Security Research Group. (2022). Let's Build a Better Internet, 2022 Annual Report. Available at: https://www.abetterinternet.org/documents/2022-ISRG-Annual-Report.pdf.