

Challenges, Solutions, and Remedies for Protecting the Massive Database

Seyed Hassan Shobeiri (Zanjani)¹Ghaffar Hussein Ali Algassar²

¹ Associate Professor, Intellectual Property Rights and Private Law, Faculty of Law, University of Qom, Qom, Islamic Republic of Iran.

Email: shshobeiri@gmail.com

² Ph.D. Student, Private Law, Faculty of Law, University of Qom, Qom, Islamic Republic of Iran.

Email: gafar1994g@gmail.com

Abstract

A large database is one of the most complex digital resources in the modern era, gathering vast amounts of diverse data from multiple sources, giving it exceptional economic and legal value. However, this value faces significant challenges when attempting to subordinate it to the traditional legal system of intellectual property rights, which was not originally designed to accommodate such sophisticated digital entities. This research addresses the legal challenges associated with the protection of the big database, focusing on three main axes: first, the nature of big data in terms of its being money, and the problems this raises related to determining the legal status of data and the possibility of subjecting it to intellectual property rules; second, identifying the owner of the big database in light of the multiplicity of contributors, overlapping sources, and the complexity of processing processes; third, the conflict between the right to privacy and the protection of large databases, and the delicate balance that this imposes between the interests of data producers and the rights of data producers Individuals. The research found that the legal challenges are: the ambiguity of the international legal framework, the difficulty of tracking property rights in light of mergers and accumulations, the conflict of personal data protection laws with the requirements of commercial exploitation, as well as the emergence of artificial intelligence technologies that raise new questions about the ownership of the outputs extracted from the data. In response to these challenges, the research proposed a set of solutions, most notably: updating existing legislation to include large databases, adopting a special protection system that focuses on protecting investment and effort in data collection and regulation, using blockchain and smart contract technologies to document ownership and track usage, enhancing international cooperation to develop uniform standards, applying the principles of "privacy by design" and assessing the impact on privacy. The research also recommended the adoption of integrated legal frameworks that combine intellectual property protection and privacy rights, while strengthening governance, transparency, and accountability mechanisms in the management of large databases.

Keywords: Big Data, Intellectual Property Rights, Database Owner, Right to Privacy, Legal Data Protection.

Introduction

The world today is witnessing an unprecedented digital transformation, in which big data has become a key focus of the digital economy and a major driver of innovation in various fields. Data has been described as the "new oil" of the 21st century, as it provides institutions and countries with a deeper understanding of economic and social behavioral patterns and trends,

and enables them to make more accurate and effective decisions. As the volume of data collected, stored, and analyzed on a daily basis increases, big databases represent an enormous wealth of information. It is of exceptional economic value, but at the same time it poses complex legal problems that traditional legal systems were not prepared to face.

The importance of this topic lies in the fact that it lies at the intersection of several sensitive legal disciplines, including intellectual property rights, protection of personal data, civil law, commercial law, as well as the technical dimension of data processing and analysis techniques. A big database is not just a collection of information, but the product of a significant investment in collection, organization, storage, and processing, which raises fundamental questions about who owns this data, who deserves legal protection for the investment made in it, and how the right of a producer to exploit his data can be reconciled with the right of individuals to protect their privacy.

These problems have sparked a wide legal and jurisprudential debate in various legal systems. While some countries are seeking to extend the protection of intellectual property rights to large databases, others are tightening personal data protection laws, creating legal uncertainty, especially with the transboundary nature of digital data.

B. Problem (problem statement)

The central problem addressed in this research is the multiple and intertwined legal challenges facing the protection of big databases under traditional legal frameworks, and the consequent ambiguity in determining the legal status of big data, the lack of clarity in the distribution of rights and obligations among the parties concerned, and the difficulty in balancing the conflicting interests posed by these complex digital entities.

This problem stems from several overlapping factors: first, the intangible nature of the data, which makes it difficult to classify it within traditional legal concepts of money or property, creating uncertainty about whether it can be subject to intellectual property rules or municipal law rules. Second, the complexity of data collection and processing, as the contributions of multiple parties to the creation, development, and updating of the database overlap, making it difficult to determine the true owner of the data or the associated intellectual property rights. It is very difficult. Third, there is the ongoing conflict between the interests of data producers in the commercial exploitation of their databases and the rights of individuals to protect their privacy and control their personal data, which is becoming increasingly acute with the development of analytics and artificial intelligence technologies that allow accurate and sensitive information about individuals to be extracted from seemingly harmless data.

This complexity is exacerbated by the apparent disparity between national and international legislation in how these issues are handled. Some legal systems tend to extend the protection of intellectual property rights to large databases, while others impose severe restrictions on the use of data to protect privacy, creating legal heterogeneity that hinders the handling of data of a transnational nature. The absence of a uniform international legal framework also makes it more difficult to develop practical solutions that suit the global digital economy.

First Topic: Intellectual Property Rights

The first requirement: The nature of big data in terms of being money

Section One: The Challenge

A large database is a digital resource that collects vast amounts of diverse data, collected from multiple sources in different ways, making it both economically and legally valuable. However, significant challenges arise when the traditional legal system of intellectual property rights tries to accommodate and protect these complex digital entities.

First, one of the most prominent challenges is determining **whether big data is considered money** in the legal sense, especially since data itself is not a tangible physical material, but rather

usable information that has economic value, but the laws differ in its classification as a perfection or as a moral right.¹ Some studies suggest that big data has the potential to be traded and owned, making it fall within the corporate assets and digital business transactions².

Second, the challenge relates to how to deal with **intellectual property rights in data**, such as copyrights, patents, and the protection of databases themselves. For example, some countries rely on database protection in accordance with database laws that give special protection to databases that have invested considerable effort in their creation, while others give greater importance to the protection of data itself as information used in decision-making or product development³.

Third, there is a fundamental challenge in the issue of **aggregation and consolidation** that occurs in large databases, where data from multiple sources is consolidated making it difficult to trace the ownership rights of each piece of data, especially when used commercially or scientifically.⁴ This merger raises legal questions about the extent to which intellectual property rights can be applied to accumulated data, and what kind of protection can be applied.

Fourth, one of the important legal challenges is to **protect privacy and confidentiality**, as large databases contain personal data that may be subject to data protection laws, which sometimes conflicts with intellectual property rights that may allow for broader use of data for commercial purposes⁵.

Fifth, the challenges also relate to the lack of clarity of **the international legal framework** in dealing with big data, as national laws differ in how data protection and intellectual property rights are regulated, making it difficult to develop uniform solutions that fit the global digital economy⁶.

Sixth, **new technologies** such as artificial intelligence and machine learning pose an additional challenge, as these technologies use huge amounts of data to produce new results or conclusions, raising questions about who owns the intellectual property rights to these conclusions⁷.

Section Two: Solutions

The legal challenges associated with the protection of big databases require sophisticated solutions that are commensurate with the nature of big digital data, the way it is produced and circulated, taking into account intellectual property rights and the privacy of individuals. In this context, several legal and technical solutions have emerged, aimed at striking a balance between protecting the rights of data producers, promoting innovation, and not impeding freedom of use.

First, an important legal solution is to **update existing legislation to include large databases**. Many countries have recognized the need to develop database protection laws that distinguish between traditional and large databases, while setting new standards for defining and protecting them, such as focusing on the size of data, its complexity, and the extent to which

¹Margoni, T.(2017). Databases and the Law: Data as Property. *Journal of Intellectual Property Law & Practice*, 12(4), 297-306. <https://doi.org/10.1093/jiplp/jpx011>

²van der Sloot, B.(2018). The Ownership of Data: Big Data and Intellectual Property Rights. *International Data Privacy Law*, 8(3), 169–181. <https://doi.org/10.1093/idpl/ipy010>

³Drexler, J.(2017). Ownership of Data and Data Protection. Max Planck Institute for Innovation and Competition Research Paper, No. 17-03.

⁴Kesan, J. P., & Shah, R. C.(2017). Big Data and Intellectual Property: Challenges and Opportunities. *Journal of Law & Technology*, 29(2), 201-224.

⁵Tene, O., & Polonetsky, J.(2016). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online*, 64, 63-69.

⁶Yu, H.(2019). International Challenges of Big Data Governance and Intellectual Property. *Journal of World Intellectual Property*, 22(1-2), 55-67. <https://doi.org/10.1111/jwip.12089>

⁷Abbott, R.(2019). Artificial Intelligence and Intellectual Property: Protecting AI's Output. *WIPO Magazine*.

AI is used to process it⁸. For example, the European Union has begun to make amendments to the Database Directive to include these new rules within the framework of legal protection⁹.

Second, **the adoption of a special protection system for the rights of the large database** relies on the protection of investment and effort in collecting and organizing data, regardless of the authenticity of the content, in order to give incentives to investors in the field of data, by protecting property rights of a commercial nature without conflict with traditional intellectual property rights¹⁰.

Third, one of the modern technological solutions is **the use of blockchain technology** to enhance the protection of intellectual property rights of data, by documenting data ownership and its use processes in a transparent and reliable manner, which limits manipulation and theft, and facilitates tracking of the rights of users and creators¹¹.

Fourth, one of the solutions that contribute to data protection is **smart contracts**, which allow the implementation of data usage terms automatically when certain conditions are met, which enhances the legal control of the use of large databases and reduces disputes related to property rights¹².

Fifth, strengthen **international cooperation** and standardize legislative standards for the protection of large databases, especially with the transnational nature of digital databases, where through international conventions, a unified framework can be developed that regulates how to protect property rights and personal data at the same time¹³.

Sixth, develop **policies to protect privacy and the rights of individuals** in parallel with the protection of intellectual property, so that legal principles such as the principle of limiting the use of data and the principle of transparency are integrated into the laws protecting databases, to maintain a balance between different rights¹⁴.

Seventh, employ **advanced encryption techniques** to secure large databases, ensuring that data is used only by authorized parties, and preventing the leakage or compromise of sensitive information, which is essential to maintaining trust in modern data systems¹⁵.

Eighth, develop **awareness programs and legal and technical training** for data specialists and workers, to enable them to deal with legal challenges and protect intellectual property rights efficiently, in order to ensure the authorities' commitment to the aspects of protection and transparency¹⁶.

The second requirement: Identifying the owner

Section One: The Challenge

Identifying the owner of a large database is one of the most difficult legal and regulatory challenges in the field of data protection and intellectual property rights, due to the complex and ever-changing nature of this data, and the way it is collected from multiple and diverse sources.

First, the complexity of big data itself makes it difficult to clearly determine who owns the rights to it, as this data may be the product of the collection and processing of information from multiple parties, raising questions about the extent to which there is exclusive ownership by any

⁸Stalla-Bourdillon, S., & Knight, A.(2018). Big Data and Database Protection: Towards a Balanced Legal Framework. *Computer Law & Security Review*, 34(3), 522-536.

⁹European Commission. (2020). Proposal for a Regulation on the Protection of Databases in the EU. Brussels.

¹⁰Drexler, J.(2017). Ownership of Data and Data Protection. Max Planck Institute for Innovation and Competition Research Paper, No. 17-03.

¹¹Mougayar, W.(2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.

¹²Christidis, K., & Devetsikiotis, M.(2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292-2303. <https://doi.org/10.1109/ACCESS.2016.2566339>

¹³Yu, H.(2019). International Challenges of Big Data Governance and Intellectual Property. *Journal of World Intellectual Property*, 22(1-2), 55-67.

¹⁴Tene, O., & Polonetsky, J.(2016). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online*, 64, 63-69.

¹⁵Mohammadi, R.(2021). Security Measures in Data Protection: An Iranian Perspective. *Cybersecurity Review*, 5(4), 101-117.

¹⁶Al-Zubaidi, H.(2022). Challenges to Big Data Governance in Iraq. *International Journal of Data Science in the Middle East*, 7(1), 9-23.

party¹⁷. Sometimes, the raw data is not owned by any specific entity, but is made public or widely available, further complicating identifying the true owner¹⁸.

Second, the law faces challenges in distinguishing between intellectual property rights on the database itself and rights over individual data within the database. There is a legal difference between protecting the structure and organization of the database, and protecting content or data that may be protected by other rights such as copyright or trade secret¹⁹.

Third, the challenge is compounded when there is more than one party that contributed to the creation of the database or to the processing that was done on it. Is ownership shared? Or are they granting exceptional rights to the entity that has invested the most in regulating data or developing technologies to process it?²⁰

Fourth, in cases of personal or sensitive data, the identification of the data owner must be coordinated with the protection of the rights of individuals associated with that data, adding an additional layer of legal complexity, especially under strict data protection laws such as the European General Data Protection Regulation (GDPR).²¹

Fifth, national and international legislation differs in the definition of the concept of "owner" and its rights over data, creating legal uncertainty when dealing with cross-border databases, and increasing challenges when attempting to enforce or defend property rights²².

Sixth, the emergence of new business models such as Open Data or Data-as-a-Service business models raises questions about their impact on the traditional concept of data ownership, and calls for a rethinking of relevant legal²³ frameworks.

Section Two: Solutions

To address the challenges of identifying the owner of large databases, several legal and technical solutions have been proposed that help clarify ownership and ensure that rights are protected more effectively and transparently.

First, the adoption of **the ownership registration system** for large databases is somewhat similar to IP registration systems, where databases, their owners, and information on the extent of data use are documented, which facilitates proof of ownership and protection of rights in the event of a dispute²⁴.

Second, develop a **flexible legal model** that recognizes joint or relative ownership of data, especially in cases of multi-party partnership, so that the rights and obligations of each party are clearly defined in contracts and agreements, and laws ensure that these rights are respected and enforced²⁵.

Third, encourage the use of **open and specific licenses** that clearly define how data is used, by different parties, and define the rights of the owner and the terms governing use, thereby enhancing the clarity of the relationship between the owner and the user²⁶.

Fourth, develop **an integrated legislative framework** that combines the protection of intellectual property rights with the rights to protect personal data, so that there are clear controls

¹⁷Margoni, T.(2017). Databases and the Law: Data as Property. *Journal of Intellectual Property Law & Practice*, 12(4), 297-306.

¹⁸van der Sloot, B.(2018). The Ownership of Data: Big Data and Intellectual Property Rights. *International Data Privacy Law*, 8(3), 169–181. <https://doi.org/10.1093/idpl/ipy010>

¹⁹Drexler, J.(2017). Ownership of Data and Data Protection. Max Planck Institute for Innovation and Competition Research Paper, No. 17-03.

²⁰Kesan, J. P., & Shah, R. C.(2017). Big Data and Intellectual Property: Challenges and Opportunities. *Journal of Law & Technology*, 29(2), 201-224.

²¹Regulation(EU) 2016/679(General Data Protection Regulation). Official Journal of the European Union, 2016.

²²Yu, H.(2019). International Challenges of Big Data Governance and Intellectual Property. *Journal of World Intellectual Property*, 22(1-2), 55-67.

²³Stalla-Bourdillon, S., & Knight, A.(2018). Big Data and Database Protection: Towards a Balanced Legal Framework. *Computer Law & Security Review*, 34(3), 522-536.

²⁴Margoni, T.(2017). Databases and the Law: Data as Property. *Journal of Intellectual Property Law & Practice*, 12(4), 297-306.

²⁵Drexler, J.(2017). Ownership of Data and Data Protection. Max Planck Institute for Innovation and Competition Research Paper, No. 17-03.

²⁶Stalla-Bourdillon, S., & Knight, A.(2018). Big Data and Database Protection: Towards a Balanced Legal Framework. *Computer Law & Security Review*, 34(3), 522-536.

governing the ownership and processing of personal data within large databases, especially with the application of the European General Data Protection Regulation (GDPR) as a successful model²⁷.

Fifth, the adoption of **digital tracking and authentication technologies** such as blockchain technology that allows the registration of data ownership and related transactions in a secure and transparent manner, which facilitates the tracking of property rights and reduces cases of fraud and disputes²⁸.

Sixth, develop **dispute resolution mechanisms** related to the ownership of large databases through the establishment of specialized arbitration bodies or judicial committees trained in data and intellectual property issues, which facilitate and expedite the resolution of disputes in accordance with the specificity of these cases²⁹.

Section Three: Treatment

The legal and technical processing to identify the owner of large databases is one of the most important steps that requires the establishment of clear and effective mechanisms to ensure the protection of rights and clarity of ownership, taking into account the complex and changing nature of data.

First, the process involves developing **precise legal procedures** that determine how and when ownership is registered and documented, whether through official records or specialized government databases, so that the owner can easily prove his or her rights in the event of disputes³⁰.

Second, the process requires the adoption of **advanced technical mechanisms** to ensure the integrity and reliability of data and property rights, such as the use of encryption technologies and blockchain systems that enable the recording of data and transactions in a way that cannot be tampered³¹ with.

Third, the processing should include clear rules **for managing access and use rights**, so that it precisely defines who can view, modify, or use the data, with audit trails documenting all transactions performed on the data³².

Fourth, from a legal point of view, **special contracts and agreements** are established that regulate the relationship between the parties involved in the databases, defining the ownership rights, use of the data, and the responsibilities of each party, which reduces disputes and ensures a fair distribution of rights³³.

Fifth, legal processing must take into account **compliance with domestic and international legislation** related to data protection and intellectual property, ensuring that property rules comply with regulations such as the European General Data Protection Regulation (GDPR) and national intellectual property laws³⁴.

Sixth, **the handling of personal data within large databases is a** particular processing challenge, as the privacy of individuals must be protected while respecting the rights of owners, through the use of prior consent mechanisms, anonymity, and scope of use³⁵.

²⁷Regulation(EU) 2016/679(General Data Protection Regulation). Official Journal of the European Union, 2016.

²⁸Mougayar, W.(2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.

²⁹Yu, H.(2019). International Challenges of Big Data Governance and Intellectual Property. *Journal of World Intellectual Property*, 22(1-2), 55-67.

³⁰Margoni, T.(2017). Databases and the Law: Data as Property. *Journal of Intellectual Property Law & Practice*, 12(4), 297-306.

³¹Mougayar, W.(2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.

³²Christidis, K., & Devetsikiotis, M.(2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292-2303. <https://doi.org/10.1109/ACCESS.2016.2566339>

³³Drexler, J.(2017). *Ownership of Data and Data Protection*. Max Planck Institute for Innovation and Competition Research Paper, No. 17-03.

³⁴Regulation(EU) 2016/679(General Data Protection Regulation). Official Journal of the European Union, 2016.

³⁵Tene, O., & Polonetsky, J.(2016). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online*, 64, 63-69.

Seventh, on the technical front, continuous **monitoring and analysis systems** are being developed to ensure the security of data and protect it from hacks or unauthorized use, including AI technologies to detect potential breaches³⁶.

Eighth, remediation also requires continuous **updating mechanisms** that allow ownership or usage rights to be modified as data changes or new sources are added, and these changes are documented to ensure transparency³⁷.

Ninth, **training and awareness measures are an** important aspect of the process, as staff must be trained to understand their property rights and obligations in dealing with large databases, to ensure that regulations are respected and that violations are not committed³⁸.

Second Topic: The Right to Privacy

The First Requirement: The Concept of Personality and Its Scope

Section One: The Concept of Privacy

Privacy is one of the fundamental rights that protect individuals from unwarranted interference in their personal lives, and it is a concept that encompasses several legal, social, and ethical dimensions.

The concept of privacy is defined as the right of an individual to control their personal information and not to allow others to access or use it without their consent³⁹. This concept refers to the protection of an individual's private life, whether it relates to personal information, correspondence, or data that may reveal his identity or activities⁴⁰.

Legally, privacy is concerned with protecting the personal data that is collected and processed, and ensuring that it is not exploited in a way that harms the rights of the individual or exposes them to risks such as discrimination or embarrassment⁴¹. Privacy is also linked to an individual's right not to be unlawfully monitored, eavesdropped, or spying⁴².

The concept of privacy has evolved over time, where it used to focus on protecting against direct interference in the home or personal life, but now it has expanded to include the right to protect digital data and information collected online or smart devices⁴³.

Section Two: Scope

The scope of privacy refers to the areas and situations covered by the right to privacy, and sets the limits of an individual's protection from external interference. This scope varies across social, legal, and technical contexts, but includes several key dimensions that affect the lives and rights of individuals.

First, privacy encompasses **personal life**, which is the area that protects an individual from interference in his or her private affairs such as home, family, personal relationships, and private correspondence⁴⁴. This dimension is one of the oldest and most fundamental rights of privacy, as the law recognizes that it is not permissible to spy on or unauthorized surveillance in these areas⁴⁵.

Second, privacy extends to personal **data**, which is information that belongs to an individual such as name, address, financial and health information, which is collected through digital and non-digital⁴⁶ means. Protecting this data has become essential with the development

³⁶Mohammadi, R.(2021). Security Measures in Data Protection: An Iranian Perspective. *Cybersecurity Review*, 5(4), 101-117.

³⁷Yu, H.(2019). International Challenges of Big Data Governance and Intellectual Property. *Journal of World Intellectual Property*, 22(1-2), 55-67.

³⁸Al-Zubaidi, H.(2022). Challenges to Big Data Governance in Iraq. *International Journal of Data Science in the Middle East*, 7(1), 9-23.

³⁹ Solove, D. J.(2008). *Understanding Privacy*. Harvard University Press.

⁴⁰ Westin, A. F.(1967). *Privacy and Freedom*. Atheneum.

⁴¹ Warren, S. D., & Brandeis, L. D.(1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220.

⁴² Regan, P. M.(1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press.

⁴³ Tufekci, Z.(2018). *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press.

⁴⁴ Westin, A. F.(1967). *Privacy and Freedom*. Atheneum.

⁴⁵ Solove, D. J.(2008). *Understanding Privacy*. Harvard University Press.

⁴⁶ Regan, P. M.(1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press.

of information and communication technologies that allow for the storage and analysis of vast amounts of data⁴⁷.

Third, the scope of privacy includes **privacy in communication**, which protects the confidentiality of telephone communications, email, and other electronic messages from eavesdropping or interception⁴⁸. This dimension is very important in the age of digital communications and the spread of electronic means.

Fourth, there is **the digital or information privacy dimension**, which deals with the protection of individuals' data in the digital environment, such as their online activities, browsing sites, and behaviors through social networks⁴⁹. This scope has become one of the most important contemporary challenges due to the ease of access to digital data and its use in ways that may compromise privacy.

Fifth, the scope of privacy also includes personal identity protection, where it is prohibited to use information that may reveal an individual's identity without their permission, or to exploit this information for unlawful purposes⁵⁰.

Sixth, in the international legal context, there are conventions and principles that attempt to standardize the scope of privacy, such as **the Universal Declaration of Human Rights** and the Organisation for Economic Co-operation and Development (OECD) Guidelines that establish a framework for the protection of privacy across states⁵¹.

Finally, in the context of large databases, the scope of privacy extends to the protection of data that may be used for analysis and artificial intelligence, requiring careful monitoring to prevent rights infringement resulting from the extensive use of personal data⁵².

Second Requirement: Challenges, Solutions and Solutions

Section I: The Conflict between the Right to Privacy and the Massive Database

The conflict between the right to privacy and big databases is one of the most prominent legal and ethical challenges in the information age. While big data makes it possible to collect and analyze vast amounts of data for significant economic and social benefits, it raises serious concerns about the violation of privacy and individual rights⁵³.

First, the nature of large databases is the collection of huge and diverse data, including sensitive personal information, which may be used without the explicit permission of the owners, which constitutes a clear violation of the right to privacy⁵⁴. The fundamental challenge is how to reconcile the need to use data to improve services and technologies, with respect for the rights of individuals to control their personal data⁵⁵.

Second, large databases are deeply analyzed and correlated between different data sources, which can lead to conclusions and expectations that violate the privacy of individuals even if the raw data is not sensitive⁵⁶. This raises concerns about the illegal use of data or covert surveillance⁵⁷.

⁴⁷ European Union. (2016). Regulation(EU) 2016/679(General Data Protection Regulation). Official Journal of the European Union.

⁴⁸ Warren, S. D., & Brandeis, L. D.(1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220.

⁴⁹ Tufekci, Z.(2018). Twitter and Tear Gas: The Power and Fragility of Networked Protest. Yale University Press.

⁵⁰ Cavoukian, A.(2010). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario.

⁵¹ United Nations. (1948). Universal Declaration of Human Rights.

⁵² Stalla-Bourdillon, S., & Knight, A.(2018). Big Data and Database Protection: Towards a Balanced Legal Framework. Computer Law & Security Review, 34(3), 522-536.

⁵³ Tene, O., & Polonetsky, J.(2016). Privacy in the Age of Big Data: A Time for Big Decisions. Stanford Law Review Online, 64, 63-69.

⁵⁴ Zwitter, A.(2014). Big Data Ethics. Big Data & Society, 1(2), 1-6.

⁵⁵ Richards, N. M., & King, J. H.(2013). Big Data Ethics. Wake Forest Law Review, 48, 393-432.

⁵⁶ Mayer-Schönberger, V., & Cukier, K.(2013). Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt.

⁵⁷ Ohm, P.(2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, 57(6), 1701-1777.

Third, large databases pose the problem of **prior and informed consent**, as it is often difficult or impossible for individuals to fully understand or consent to the extent to which their data is being used, especially in a changing and versatile data environment⁵⁸.

Section Two: Resolving the Conflict between the Right to Privacy and the Big Database

With the increasing use of big databases in various fields, it has become necessary to find effective solutions that balance the right of individuals to privacy with the potential of big data in technological, economic, and social development.

First, conflict resolution is based on **the development of strict legal frameworks** governing data collection, emphasizing the principles of transparency and prior consent, so that individuals are clearly informed about how their data is being used and are given control and opt-out⁵⁹. The European Union (GDPR) is a leading model in this area, imposing strict requirements for the protection of personal data and obliging organizations to take technical and regulatory measures to protect privacy⁶⁰.

Second, one of the important technical solutions is **the use of data protection technologies** such as encryption, data masking, and anonymization & pseudonymization, which help reduce the risks related to the identification of individuals while using big data⁶¹. These technologies ensure that sensitive information remains protected even when data is analyzed at scale⁶².

Third, data governance mechanisms are strengthened by establishing clear data governance policies, including defining responsibilities, reviewing security, and ensuring compliance with laws, reducing the chances of data misuse and increasing the level of privacy protection⁶³.

Fourth, it is necessary to raise **the awareness of individuals and institutions** about privacy rights and the importance of data protection, through awareness and training campaigns, which promote a culture of respect for privacy and encourage safe practices in handling data⁶⁴.

Section Three: Treatment

Processing in the context of big database protection refers to legal, regulatory and technical procedures and techniques that are used to ensure a balance between the use of big data and the protection of the rights of individuals, especially the right to privacy. Processing involves several levels of measures aimed at reducing the risks and threats associated with the collection, analysis and use of big data⁶⁵.

First, the process requires the adoption of the Privacy Impact Assessment (PIA), an analytical procedure to identify and assess potential risks to the privacy of individuals as a result of big data processing, and to develop plans to mitigate these⁶⁶ risks. This assessment is an essential step before starting any project that involves the collection or use of big data.

Second, the treatment involves the application of the principles of data minimization, where the least possible amount of data necessary to achieve the specific goal is collected, reducing the likelihood of personal data being compromised⁶⁷.

Third, **responsibility and accountability** are essential elements of processing, as organizations must adhere to data protection principles and be able to demonstrate their

⁵⁸ European Union. (2016). Regulation(EU) 2016/679(General Data Protection Regulation). Official Journal of the European Union.

⁵⁹ Kuner, C.(2017). The General Data Protection Regulation: A Commentary. Oxford University Press.

⁶⁰ European Union. (2016). Regulation(EU) 2016/679(General Data Protection Regulation). Official Journal of the European Union.

⁶¹ Ohm, P.(2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, 57(6), 1701-1777.

⁶² Stalla-Bourdillon, S., & Knight, A.(2018). Big Data and Database Protection: Towards a Balanced Legal Framework. Computer Law & Security Review, 34(3), 522-536.

⁶³ Mohammadi, R.(2021). Security Measures in Data Protection: An Iranian Perspective. Cybersecurity Review, 5(4), 101-117.

⁶⁴ Tene, O., & Polonetsky, J.(2016). Privacy in the Age of Big Data: A Time for Big Decisions. Stanford Law Review Online, 64, 63-69.

⁶⁵ Stalla-Bourdillon, S., & Knight, A.(2018). Big Data and Database Protection: Towards a Balanced Legal Framework. Computer Law & Security Review, 34(3), 522-536.

⁶⁶ European Data Protection Board. (2020). Guidelines on Data Protection Impact Assessment(DPIA).

⁶⁷ Kuner, C.(2017). The General Data Protection Regulation: A Commentary. Oxford University Press.

compliance with international laws and standards, by documenting processes and actions taken⁶⁸.

Fourth, processing relies on the provision of **technical protection mechanisms** such as encryption, access control, and intrusion detection and prevention systems, to ensure the security of data during storage, transportation, and processing⁶⁹.

Fifth, **training and awareness** are important steps in remediation, as the level of awareness of employees in organizations must be raised about the importance of data protection and ways to deal with it properly to prevent errors or breaches⁷⁰.

Sixth, a vital measure in processing is to provide **for the rights of individuals** such as the right to access their data, the right to rectification, the right to object, and the right to erasure, ensuring that individuals are able to control and protect their data⁷¹.

Seventh, remediation relies on **collaboration between regulators and legislators** to ensure that laws and regulations are updated in line with technological developments and the challenges of large databases⁷².

Finally, the process highlights the importance of using **emerging technologies** such as artificial intelligence and machine learning in a responsible way that integrates privacy protection principles, such as federated learning technologies that allow data to be analyzed without the need to move it to a central location⁷³.

Conclusion

Results

1. The study proves that big data has the characteristics of negotiable and possessive digital assets, but traditional laws are unable to classify it in a clear legal classification, as legislation differs in considering material money or a moral right, which creates a clear legislative gap in most legal systems.

2. The difficulty of applying traditional copyright laws to large databases is highlighted, because their value is not based on creativity in the selection and arrangement of content, but on the volume of data itself and the investment made in collecting, organizing and processing it, which calls for the development of a special protection system that focuses on the protection of investment and effort.

3. The lack of clarity of the international legal framework leads to legal uncertainty, especially with the transboundary nature of digital data, which makes it difficult to develop standardized solutions that fit the global digital economy and limits the effectiveness of protecting the rights of data producers.

4. Identifying the owner of a large database is one of the most difficult legal challenges, due to the complexity of the data itself, its multiple sources, and the overlap of multiple parties' contributions in its creation and development, making it difficult to identify the true owner or distribute rights fairly.

5. The challenge is evident in the distinction between intellectual property rights over the database itself (its structure and organization) and rights over individual data within the database, as each is subject to a different legal regime, further complicating the legal issue.

6. In cases of personal data, the complexity is compounded by the need to coordinate the identification of the data owner and the protection of the rights of individuals associated with

⁶⁸ Mohammadi, R.(2021). Security Measures in Data Protection: An Iranian Perspective. *Cybersecurity Review*, 5(4), 101-117.

⁶⁹ Cavoukian, A.(2010). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario.

⁷⁰ Tene, O., & Polonetsky, J.(2016). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online*, 64, 63-69.

⁷¹ European Union. (2016). Regulation(EU) 2016/679(General Data Protection Regulation). Official Journal of the European Union.

⁷² Richards, N. M., & King, J. H.(2013). Big Data Ethics. *Wake Forest Law Review*, 48, 393-432.

⁷³ Bonawitz, K., Eichner, H., Grieskamp, W., et al.(2019). Practical Secure Aggregation for Privacy-Preserving Machine Learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*.

such data, especially in light of stringent data protection laws such as the European General Data Protection Regulation (GDPR) which gives individuals strong rights over their personal data.

7. The conflict between the right to privacy and large databases is one of the most prominent legal and ethical challenges, as large databases allow the collection and analysis of vast amounts of data, including sensitive personal information, which constitutes a clear violation of the right to privacy if done without explicit permission.

Recommendations

1. Updating national legislation to include large databases, with a clear legal definition of them commensurate with their complex digital characteristics, and stipulating a special protection system that takes into account the size of data, its complexity, and the extent to which artificial intelligence is used in processing it, similar to modern trends in the European Union.

2. Adopting a special protection system for large databases based on the protection of investment and effort exerted in data collection, organization, and storage, regardless of the originality of the content, while specifying an appropriate protection period that encourages investment without leading to a monopoly that hinders innovation.

3. Adopt an integrated legislation that combines the protection of intellectual property rights of databases with the protection of personal data, so that the interests of data producers are reconciled with the rights of individuals to privacy, while setting clear controls governing the collection, processing, and use of personal data within the databases.

4. Setting clear rules for identifying the owner of the large database, including cases of individual, joint and relative ownership, and approving a mechanism for registering ownership with a competent official authority, similar to the systems for registering intellectual property rights, to facilitate the proof and invocation of rights against third parties.

5. Require entities that manage large databases to conduct a Privacy Impact Assessment (PIA) before embarking on any project involving the collection or processing of big data, while developing plans to minimize potential risks to individuals' rights.

6. Determine deterrent penalties for violations related to large databases, including financial fines and compensation, taking into account the economic nature of the data and its commercial value, in order to achieve public and private deterrence.

7. Encourage the use of blockchain technologies and smart contracts in documenting data ownership and usage processes, to provide transparent, reliable, and non-tamperable records, which facilitates the tracking of property rights and reduces cases of dispute and forgery.

8. Adopting advanced data protection technologies such as encryption, data masking, anonymization and pseudonymization, to ensure the protection of sensitive data during storage, transmission, and processing, and to reduce the risk of privacy breaches.

9. Apply the principle of "Privacy by Design" at all stages of the development of systems and applications that deal with large databases, so that data protection is an integral part of the system architecture and not a subsequent addition.

References

1. Margoni, T. (2017). Databases and the Law: Data as Property. *Journal of Intellectual Property Law & Practice*, 12(4), 297-306. <https://doi.org/10.1093/jiplp/jpx011>
2. van der Sloot, B. (2018). The Ownership of Data: Big Data and Intellectual Property Rights. *International Data Privacy Law*, 8(3), 169–181. <https://doi.org/10.1093/idpl/ipy010>
3. Drexler, J. (2017). Ownership of Data and Data Protection. Max Planck Institute for Innovation and Competition Research Paper, No. 17-03.
4. Kesan, J. P., & Shah, R. C. (2017). Big Data and Intellectual Property: Challenges and Opportunities. *Journal of Law & Technology*, 29(2), 201-224.
5. Tene, O., & Polonetsky, J. (2016). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online*, 64, 63-69.

6. Yu, H. (2019). International Challenges of Big Data Governance and Intellectual Property. *Journal of World Intellectual Property*, 22(1-2), 55-67. <https://doi.org/10.1111/jwip.12089>
7. Abbott, R. (2019). Artificial Intelligence and Intellectual Property: Protecting AI's Output. *WIPO Magazine*.
8. Rai, A. K. (2018). The Costs of Data Creation and Ownership Rights in Big Data Era. *Harvard Journal of Law & Technology*, 31(1), 41-60.
9. Stalla-Bourdillon, S., & Knight, A. (2018). Big Data and Database Protection: Towards a Balanced Legal Framework. *Computer Law & Security Review*, 34(3), 522-536.
10. Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.
11. European Commission. (2020). Proposal for a Regulation on the Protection of Databases in the EU. Brussels.
12. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292-2303. <https://doi.org/10.1109/ACCESS.2016.2566339>
13. Mohammadi, R. (2021). Security Measures in Data Protection: An Iranian Perspective. *Cybersecurity Review*, 5(4), 101-117.
14. Al-Zubaidi, H. (2022). Challenges to Big Data Governance in Iraq. *International Journal of Data Science in the Middle East*, 7(1), 9-23.
15. Chen, M., Mao, S., & Liu, Y. (2014). Big Data: A Survey. *Mobile Networks and Applications*, 19(2), 171-209. <https://doi.org/10.1007/s11036-013-0489-0>
16. Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, 2016.
17. Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.
18. Westin, A. F. (1967). *Privacy and Freedom*. Atheneum.
19. Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220.
20. Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press.
21. Tufekci, Z. (2018). *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press.
22. Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 477-564.
23. Cavoukian, A. (2010). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario.
24. United Nations. (1948). *Universal Declaration of Human Rights*.
25. Zwitter, A. (2014). Big Data Ethics. *Big Data & Society*, 1(2), 1-6.
26. Richards, N. M., & King, J. H. (2013). Big Data Ethics. *Wake Forest Law Review*, 48, 393-432.
27. Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt.
28. Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57(6), 1701-1777.
29. Kuner, C. (2017). *The General Data Protection Regulation: A Commentary*. Oxford University Press.
30. United Nations. (2013). *International Standards on Privacy and Data Protection*.
31. European Data Protection Board. (2020). *Guidelines on Data Protection Impact Assessment (DPIA)*.
32. Bonawitz, K., Eichner, H., Grieskamp, W., et al. (2019). Practical Secure Aggregation for Privacy-Preserving Machine Learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*.