

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

Threats Posed by Artificial Intelligence to the Right to Privacy

Zakaria Guittoun ^{1*}, Abdelrahman Al-Sanousi²

¹Faculty of Islamic Sciences, El Kharrouba, University of Algiers 1, (Algeria) -
z.guittoun@univ-alger.dz

²Faculty of Law, University of Algiers 1, (Algeria), -aassanou@gmail.com

Date of send: 2026/03/03	date of acceptance: 01/05/2026	Date of Publication: 01/06/2026
--------------------------	--------------------------------	---------------------------------

***Corresponding author**

Abstract

The rapid advancement of artificial intelligence (AI) technologies has profoundly transformed contemporary societies, generating unprecedented benefits while simultaneously posing significant legal and ethical challenges. Among the most pressing concerns is the growing threat to the right to privacy, a fundamental human right essential to safeguarding individual dignity and autonomy. This article examines the impact of artificial intelligence on privacy rights, focusing on key areas such as data collection without informed consent, facial recognition and mass surveillance systems, algorithmic profiling, coercive marketing, and predictive analytics.

Using a descriptive and critical analytical approach, the study explores how AI-driven systems rely on large-scale data processing and automated decision-making mechanisms that often operate in opaque and non-transparent environments. It argues that these technological developments have produced new forms of privacy intrusion that exceed traditional legal conceptions and challenge the adequacy of existing regulatory frameworks. Although national and international legislations—particularly data protection laws—have made notable progress, significant gaps remain in addressing large-scale digital surveillance and predictive algorithmic practices.

The study concludes that achieving a balance between technological innovation and privacy protection is possible, but it requires strengthened legal frameworks, enhanced algorithmic transparency, effective informed consent mechanisms, independent oversight bodies, and ethical governance aligned with fundamental human rights principles. Ultimately, safeguarding privacy in the age of artificial intelligence demands a comprehensive and proactive regulatory response that keeps pace with technological evolution.

Keywords: Artificial Intelligence (AI); Privacy; Data Protection; Facial Recognition; Mass Surveillance; Predictive Analytics; Algorithmic Transparency; Informed Consent; Digital Rights; GDPR.

Introduction:

The contemporary world is witnessing an unprecedented boom in the field of artificial intelligence, with its applications affecting various aspects of daily life, from healthcare and education to security, media, and marketing. However, this rapid technological advancement poses significant legal and ethical challenges, the most prominent of which is the threat to the right to privacy, considered one of the most fundamental personal rights that guarantee human dignity and independence.

Concerns have increased that artificial intelligence technologies, such as facial recognition systems, big data analysis, and algorithmic surveillance, have become tools for systematic intrusion into individuals' private lives, especially in the absence or weakness of regulatory and legal deterrents in some contexts.

From this standpoint, this article has been chosen to examine the impact of artificial intelligence on the right to privacy, aiming to assess the adequacy of legal frameworks in addressing these technological challenges and their ability to protect individuals from emerging violations. The article also seeks to highlight the risks and threats surrounding private life in the digital age.

Importance of the Topic

The importance of this topic stems from its position at a sensitive intersection between rapid technological advancement and the legal and ethical guarantees of human rights, which have been enshrined for decades in various international conventions and national constitutions, with the right to privacy being at the forefront. While artificial intelligence technologies are increasingly used to analyze individual behaviors and track their digital activities with unprecedented accuracy, privacy is now threatened by new forms that go beyond traditional intrusions, necessitating a reassessment of the available legal and ethical tools to protect it.

The significance of this study also lies in highlighting the global rise in the use of artificial intelligence across various fields. It aims to contribute to the scientific and jurisprudential discussions on how to regulate this technology in a way that ensures privacy protection without hindering its potential benefits.

The Problematic of the Article

With the increasing use of artificial intelligence technologies to collect, analyze, and utilize information for various purposes, the scale of the threat these technologies pose to the right to privacy has become striking. It has become possible to track individuals, monitor their behavioral patterns, and even predict their future decisions, often without their knowledge or consent. In this context, a fundamental question arises about the ability of current legal frameworks to keep up with these transformations and whether they provide genuine protection for this essential right in the digital age.

Therefore, the central issue addressed by this article is:

To what extent do artificial intelligence technologies impact the right to privacy in light of current technological developments?

This issue branches into several sub-questions, including:

- What are the main manifestations of privacy violations resulting from the use of artificial intelligence?
- A general evaluation of national and international legal frameworks in addressing these emerging violations.
- Are there gaps or deficiencies in the legal or ethical handling of this new challenge?
- How can a balance be achieved between utilizing artificial intelligence and protecting privacy?

The Methodology Adopted

This article relies on the descriptive approach to present and analyze the manifestations of privacy violations caused by artificial intelligence applications across various forms of privacy, as well as to clarify the associated technical and social contexts. The critical approach is also employed to evaluate the effectiveness of the legal and ethical frameworks and to suggest ways to develop them to address emerging challenges.

Objectives of the Article

This article aims to achieve a number of scientific and practical objectives, the most prominent of which are:

- To clarify the nature of the relationship between artificial intelligence and the right to privacy, and to explore the main threats that these modern technologies pose to this right.
- To present and analyze the legal frameworks in place for protecting privacy, both at the national and international levels, in the context of artificial intelligence.
- To propose practical recommendations for enhancing privacy protection in light of the rapidly advancing technological revolution, balancing technological development with the safeguarding of individual rights.

Concerns have increased that artificial intelligence technologies, such as facial recognition systems, big data analysis, and algorithmic surveillance, have become tools for systematic intrusion into individuals' private lives, in the absence or, rather, weakness and failure to keep up with the rapidly advancing technological evolution day by day.

Research Plan

This article is structured into two main sections, preceded by an introduction and followed by a conclusion and some recommendations, as outlined below:

- **Introduction**
- **Chapter One:** The Conceptual Framework of Artificial Intelligence and the Right to Privacy
- **Chapter Two:** Artificial Intelligence and the Threat to Privacy

THE FIRST TOPIC : The Conceptual Framework of Artificial Intelligence and the Right to Privacy

The rapid development of artificial intelligence technologies is one of the most prominent features of the digital age, as it has had a direct impact on various fields of life, especially those related to the collection and processing of personal data. This reality has raised important legal questions regarding the protection of the right to privacy in the face of these technologies' capabilities. Therefore, this chapter aims to define the concepts of artificial intelligence and privacy, as they are essential to understanding the issues raised in the next chapter

First requirement: The Concept of Artificial Intelligence

Artificial Intelligence (AI) is one of the key features of the Fourth Industrial Revolution, referring to the ability of computer systems to simulate human intelligence by analyzing data, learning from it, making decisions, and interacting intelligently with their environment¹.

AI is also defined as: "A collection of technologies commonly referred to as artificial intelligence, which now includes various types of algorithms, programs, and methods used to analyze data and are recognized as technologies capable of acting with awareness, learning, self-improvement, decision-making, and more."²

Artificial Intelligence is considered one of the most important and advanced branches of computer science, defined as "the ability of a machine to perform tasks that typically require human intelligence, such as learning, understanding, decision-making, and language processing."³

Some researchers define AI as "a collection of digital systems capable of analyzing big data and extracting cognitive patterns that are used to make decisions or provide predictions with accuracy approaching human capabilities."⁴

The European Union's Artificial Intelligence Act defines AI systems as "software developed using one or more techniques and methods capable of achieving a specific set of goals defined by humans, or generating outputs such as

content, predictions, recommendations, or decisions that affect the environments with which they interact."⁵

The European Commission defines AI as "systems that exhibit intelligent behavior by analyzing their environment and taking actions — to some extent autonomously — to achieve specific goals. AI systems can either rely entirely on software operating in the virtual world (such as voice assistants, image analysis programs, search engines, and facial recognition systems) or be integrated into physical devices (such as advanced robots, self-driving cars, drones, or Internet applications)."⁶

In general, all definitions of AI revolve around the study of how to train machines and devices to perform tasks better than humans. Thus, AI is defined as "a way to make a computer or robot controlled by a computer, or a program that thinks intelligently in the same way that smart humans think."⁷

AI is typically classified into two main types: the first is narrow AI, which focuses on performing specific tasks with high accuracy and is the most common today, including recommendation systems, voice assistants, and facial recognition technologies. The second is general AI, which is supposed to have comprehensive cognitive abilities allowing it to learn and think across multiple fields in a manner similar to the human brain, but it is still in the realm of theoretical research and has not yet been practically applied.⁸

Researchers agree that the rapid development of AI is attributed to three main factors: (big data, advanced computational power, and the development of deep learning algorithms).⁹

second requirement: The Concept of Privacy

Privacy is considered one of the most fundamental rights that guarantees individuals a secure sphere within which they may conduct their lives free from unjustified interference or surveillance. Interest in this concept has grown significantly with the tremendous technological development that has rendered personal data increasingly susceptible to collection, processing, and exploitation. Today, privacy is no longer confined to the protection of family life or personal secrets; it also encompasses the protection of digital data that reflects an individual's identity, behaviors, and choices. Accordingly, the right to privacy has become an essential pillar for safeguarding human dignity and freedom, and a fundamental condition for establishing trust in the modern digital society. Therefore, this requirement seeks to clarify the concept of privacy in general, with particular emphasis on its digital dimension.

From a linguistic perspective, privacy is closely related to the notion of secrecy, yet it is not synonymous with it. Secrecy presupposes concealment and hiddenness, whereas privacy, although it may involve a degree of concealment, can exist even in the absence of strict secrecy.¹⁰

In Arabic language dictionaries, privacy refers to that which is personal and exclusive to an individual and should not be accessed by others.

The right to privacy is not merely a social right; rather, it is also a legally and normatively recognized right established to protect the inviolability of the person, the sanctity of the home, and the confidentiality of correspondence and communications. It constitutes a foundational principle for the preservation of human dignity.

Scholars have defined privacy in various ways. Some describe it as “the individual’s authority to remain alone with his or her life and information, and to prevent others from accessing or interfering with them without consent.” Others emphasize that privacy comprises a set of rights that enable individuals to control their image, personal data, and private affairs. At the judicial level, certain legal systems—such as the French judiciary—have recognized the right to privacy through decisions of the Court of Cassation. The Court affirmed that “the right each person holds over his or her image includes its capture, preservation, reproduction, and use, and that merely photographing a person without consent—even if the image is not published—constitutes an infringement of this right and entitles the individual to claim compensation.”¹¹

It is noteworthy that legal scholars generally agree that privacy is a relative concept, which makes it difficult to formulate a universally accepted definition. Indeed, it is virtually impossible to establish a comprehensive definition suitable for all legal contexts. The relative nature of the right to privacy varies across time and place, and even within the same temporal and spatial setting depending on individual circumstances, thereby complicating the task of defining it. Nevertheless, the difficulty of defining privacy does not preclude attempts to formulate a definition based on certain guiding principles and criteria.¹²

Accordingly, privacy may be defined as:

“the individual’s right to have his or her private life and personal secrets respected, and not to be violated by individuals, institutions, or authorities without legal authorization or legitimate justification.”

THE SECOND TOPIC Artificial Intelligence and the Threat to Privacy

Artificial intelligence is one of the most significant contemporary challenges to the right to privacy, as it fundamentally relies on big data collected from users and analyzed using advanced algorithms. This raises the question posed by some researchers: How do artificial intelligence technologies violate privacy? The main manifestations of this violation can be summarized as follows:

First requirement: Data Collection Without Knowledge or Consent¹³

There are numerous applications that collect massive amounts of personal information (such as location, photos, habits, preferences, search choices, etc.) through smartphones, search engines, social media platforms, and smart cameras, without explicitly informing the user. This constitutes a clear violation of privacy.

With the introduction of artificial intelligence tools into daily civilian life, it has become essential to consider the relationship between these systems and users' right to privacy.

Some legal scholars argue that the relationship between the user and the artificial intelligence system is often classified as a contractual relationship or implicit consent (*Contrat de consentement implicite*), where consent is given by pressing "I Agree" to the terms of service. However, this does not exempt the system provider from civil responsibility if the data is used in ways that violate privacy.¹⁴

On the other hand, some scholars believe that this relationship should be classified as a tortious relationship in cases where data is used in a non-transparent environment relying on non-explainable algorithms (Black-box AI), where it is impossible to prove genuine consent or complete knowledge.¹⁵

From the perspective of protecting the right to privacy, considering pressing the "I Agree" button as explicit or implicit consent represents an overly simplistic interpretation of digital contracting. Traditional consent assumes freedom of will, full knowledge, and the ability to negotiate—conditions that are almost nonexistent in modern digital environments. Most users "agree" out of necessity due to the length or ambiguity of documents, or because the service cannot be used without that consent. Therefore, relying on this consent to justify the collection and processing of sensitive data is a breach of the principle of genuine consent that underlies civil law.

second requirement: Facial Recognition and Mass Surveillance

Artificial intelligence systems are used to analyze images and recognize faces, linking them to user data. This allows for the surveillance of individuals in both public and private spaces, sometimes without legal justification, threatening freedom of movement and expression.

Facial recognition technologies and mass surveillance structures pose a direct threat to the right to privacy because they turn public spaces into environments where individuals can be tracked, their movements recorded, and linked to personal data (such as identity records or behavioral patterns) without their explicit consent. This type of mass surveillance is not limited to monitoring suspects but includes entire populations, leading to the storage of sensitive biometric data for long periods, with the potential for misuse (e.g., selling it to the private sector or using it to suppress opposition or enforce institutional discrimination). Furthermore, the presence of cameras and automatic recognition systems may deter people from exercising their basic rights, such as freedom of expression and assembly, creating a "chilling effect" that causes certain groups (particularly minorities) to avoid certain public spaces for fear of surveillance or misidentification.¹⁶

We are at a crossroads regarding states' approaches to facial recognition surveillance. On one hand, governments in places like "the occupied entity" and the UK are exploiting advancements in plans for the widespread use of this powerful biometric technology. On the other hand, the latest draft of the European Union's AI law reveals a growing commitment to banning its use in public spaces.

Human Rights Watch joined 180 other human rights organizations and experts on September 29, 2023, calling on governments and companies to stop using facial recognition surveillance technology in public spaces and in migration and asylum contexts because it is simply too dangerous and powerful to be used without negative consequences on human rights.¹⁷

Facial recognition surveillance technology, which scans people, identifies them, and categorizes them collectively, is incompatible with international human rights law because it amounts to mass surveillance. In addition to undermining privacy rights, this technology threatens our rights to equality, non-discrimination, freedom of expression, and freedom of assembly.

Three of the world's largest tech companies have backed away from selling facial recognition technology to law enforcement amid ongoing protests against police brutality. IBM announced on Monday that it would stop selling facial recognition technology "for general purposes." Amazon announced on Wednesday that it would impose a one-year suspension on selling its facial recognition software to law enforcement agencies. Microsoft followed suit on

Thursday, saying it would not sell facial recognition technology to U.S. police forces and would not do so until legislation governing its use is passed.¹⁸

At the same time, facial recognition surveillance technology is increasingly being used by governments to monitor protests, target individuals based on their race, and suppress political opposition. Like much of the technology, it exacerbates existing structural inequalities and hits people with marginalized and vulnerable identities hardest. There is no safe use case for this technology, neither on the streets nor at the borders. We urgently need governments to intensify their efforts and ban facial recognition surveillance in these areas, and for companies to stop creating and using this powerful technology for surveillance purposes.¹⁹

Third Requirement: Algorithmic Spying, Coercive Marketing, and Predictive Analytics

AI algorithms rely on analyzing digital interactions to direct content and advertisements, which can lead to manipulation of personal choices and even influence political and social beliefs.

Predictive analytics, which invades privacy, involves using big data, statistical algorithms, and machine learning techniques to predict sensitive individual characteristics or future behaviors, even if the original data appears harmless. The main danger is that these tools can deduce highly personal information, such as sexual orientation, health conditions (such as pregnancy or a tendency for substance abuse), or mental stability, based on seemingly innocent data like social media "likes," purchase history, or even geographical location. These inferences about sensitive data are often made without the knowledge or explicit consent of the individuals involved, which constitutes a serious violation of privacy.²⁰

Predictive analytics raises numerous ethical concerns, primarily about privacy, bias, and accountability. These issues stem from how data is collected, how models are built, and how predictions are used in real-world applications. Developers need to understand these challenges to build systems that respect users' rights and avoid harm.²¹

First, privacy and consent are primary concerns. Predictive models often rely on personal data, such as location, health records, or online behavior, which users may not be aware is being collected or analyzed.²²

For example, a health app predicting disease risks may use sensitive medical data without the user's explicit understanding. Even anonymized data can sometimes be re-identified, putting individuals at risk. Developers must ensure that data collection complies with regulations such as the General Data

Protection Regulation (GDPR) and that users explicitly consent to how their data is used. Technical measures like differential privacy or data minimization can help, but transparency with users is equally important.²³

The danger of this type of analysis lies in its potential use for discrimination or manipulation of vulnerable individuals. For example, insurance companies could use health risk predictions to deny coverage or increase premiums, while advertisers could target individuals who are predicted to be going through difficult emotional times (such as the loss of a loved one) with specific offers. These predictions can also lead to the creation of "profiles" of people and use these profiles in automated decisions that affect their chances of getting a job or a loan, reflecting potential biases in the historical data used to train the models. Therefore, the ethical use of predictive analytics requires ensuring transparency, accountability, and strict protection of personal data, along with compliance with data protection regulations such as GDPR.²⁴

The debate over bias in predictive analytics exposes another, deeper, and more fundamental risk: the violation of individuals' privacy through the prediction of their personal data. We argue that inferring personal information about individuals or groups—even if they are random—can represent a privacy violation as serious as the unauthorized use of actual data. By "actual data," we mean information disclosed voluntarily by the data subject, as opposed to inferred data generated by predictive models. This situation leads to changes in social structures, creating risks to democracy and social harmony, as well as entrenched commercial marketing practices that permeate everywhere. As we will demonstrate in this article, the privacy risks arising from predictive analytics begin at the model-building stage, not just when these models are applied to real-world cases.

As a result, the methodology of predictive analytics has direct legal consequences, most notably privacy violations, discriminatory practices, and the exploitation of imbalances in informational power that hinder the exercise of individual and collective rights. However, the current legal framework—particularly the General Data Protection Regulation (GDPR) in the European Union and the Digital Services Act (DSA)—is still incapable of effectively overseeing the deep societal risks generated by predictive analytics. Automated predictions can harm individuals and entire communities.

At the same time, predictive analytics relies on a collective causal structure, as predictive systems exploit data provided by large numbers of users when they use digital services and then apply their results to targets that may not even belong to that group of data owners. Since predictive analytics can only be practiced by entities capable of owning vast amounts of user data, we consider these practices a clear manifestation of informational power imbalance.²⁵

Conclusion:

Through this study, we have reached several conclusions, summarized in the following points:

1. It has been shown that privacy is a multidimensional concept; in language, it is related to seclusion and keeping away from the eyes of others, and in legal terms, it refers to an individual's right to control their data and private life and protect it from unjustified interference.
2. The analysis demonstrated that technological advancements in artificial intelligence—particularly in data analysis, machine learning, and algorithmic decision-making—have generated new patterns of privacy threats that go beyond traditional conceptions.
3. The study revealed that data collection without knowledge or consent has become a widespread practice, enabling intelligent systems to create accurate personal profiles, which directly violates the sanctity of private life and undermines the principle of informed consent.
4. The article concluded that facial recognition technologies and mass surveillance represent some of the most dangerous forms of privacy violation because they allow for the constant tracking of individuals in both public and private spaces, enabling the creation of comprehensive surveillance patterns that may be exploited for illicit purposes.
5. The study showed that algorithmic spying, coercive marketing, and predictive analytics deepen the violation of privacy by extracting sensitive personal traits, predicting behaviors, and influencing decisions without the individual's knowledge, transforming privacy into a commercial commodity or a tool for control.
6. The world still does not fully recognize the precise risks associated with artificial intelligence or its full impact on the lives of individuals and communities. The understanding of how it is used and regulated—by governments, private institutions, or users—is still limited in grasping the scope of future challenges. Furthermore, societal and legislative responses to these transformations remain limited and inadequate to confront the rapid development of these technologies.
7. Legally, it has been demonstrated that national and international legislations have made significant progress in organizing data protection. However, several legislative gaps still exist, particularly regarding predictive algorithms and large-scale digital surveillance.
8. The findings confirm that achieving a balance between benefiting from artificial intelligence and protecting privacy is possible, but it requires strict legal regulation, the activation of ethical controls in the digital environment, and the development of clear policies for transparency and algorithmic accountability.

Recommendations:

1. Strengthen the legal framework by enacting modern legislation to regulate the use of artificial intelligence technologies, particularly in the fields of surveillance and predictive analytics.
2. Enhance algorithmic transparency by requiring companies and institutions to disclose data collection and processing mechanisms, and granting the right to understand how automated decisions are made.
3. Establish ethical and value-based controls that align with Islamic principles in protecting individual dignity and the sanctity of private life, directing their use in digital environments.
4. Develop effective mechanisms for informed consent to ensure that data is not collected or processed without the user's knowledge or consent.
5. Establish independent regulatory bodies to oversee the use of artificial intelligence and ensure compliance with privacy protection standards.
6. Invest in digital awareness to educate individuals about their rights and how to protect their data in the face of intelligent systems.
7. Adopt advanced privacy technologies, such as encryption, data minimization, and ethical algorithms, to reduce risks associated with the automated processing of information.
8. Encourage scientific research in the fields of AI ethics, digital privacy, and future technological risks.
9. Achieve a balance between benefiting from the capabilities of artificial intelligence and ensuring that fundamental rights of individuals are not compromised.

Bibliography List :

Journal article :

First: Arabic Scholarly Articles

1. **Abdelkader Rahal**, *Criminal Protection of the Right to Privacy: A Comparative Study between Islamic Sharia and Algerian Criminal Law*, PhD Dissertation in Islamic Sciences, University of Oran, 2014/2015.
2. **Fadila Berkan**, *Protection of the Right to Privacy in Algerian Legislation*, Algerian Journal of Law and Political Sciences, Vol. 10, No. 2, 2025.
3. **Ibrahim Riyad Hegazy El-Fiqi**, *The Right to Privacy in the Face of Artificial Intelligence: A Comparative Study between Egyptian Law and European Law*, Ibram Journal of Arts and Human and Social Studies, Vol. 1, No. 1, Part 7, July 2025.
4. **Mohamed Fathi Mohamed Ibrahim**, *Legislative Regulation of Artificial Intelligence Applications*, Journal of Legal and Economic Research, Issue No. 71, September 2022.

5. **Rabie Ibrahim**, *The Legal Nature of Artificial Intelligence*, Professor Researcher Journal for Legal and Political Studies, Vol. 10, No. 01, June 2025.

Second: International Scholarly Articles

1. **Nazar El Fadel**, *Facial Recognition Algorithms: A Systematic Literature Review*, Journal of Imaging, Vol. 11, No. 2, 2025, Article 58, Department of Computer Engineering, College of Computing, Fahad Bin Sultan University, Tabuk 71454, Saudi Arabia.
2. **Rainer Mühlhoff and Hannah Ruschemeier**, *Predictive Analytics and the Collective Dimensions of Data Protection*, Law, Innovation and Technology, Vol. 16, No. 1, 2024, pp. 261–292, Routledge, Taylor & Francis Group; Institute for Philosophy & Institute for Cognitive Science, University of Osnabrück, Osnabrück, Germany; Department of Law, University of Hagen, Hagen, Germany.
3. **A. Shchitova**, *Definition of Artificial Intelligence for Legal Regulation*, Proceedings of the 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020), Atlantis Press, pp. 616–620.

Third: Web-Based and Other References

1. *What Are the Ethical Concerns in Predictive Analytics?* Available at: <https://milvus.io/ai-quick-reference/what-are-the-ethical-concerns-in-predictive-analytics> (accessed on 27/11/2025).
2. *Time to Ban Facial Recognition in Public Spaces and at Borders*, Human Rights Watch, available at: <https://www.hrw.org/news/2023/09/29/time-ban-facial-recognition-public-spaces-and-borders> (accessed on 29/11/2025).
3. *Amazon, Microsoft and IBM Halt Sales of Facial Recognition Technology to Police*, Business Insider, available at: <https://www.businessinsider.com/amazon-microsoft-ibm-halt-selling-facial-recognition-to-police-2020-6>
4. Anna Bacciarelli, “Rights Groups Sound the Alarm on Mass Surveillance Technology,” 29 September 2023, 3:09 PM EDT. (consulted on: 29/11/2025/14:30) <https://www.hrw.org/news/2023/09/29/time-ban-facial-recognition-public-spaces-and-borders>.

5. Nazar El Fadel, *Facial Recognition Algorithms: A Systematic Literature Review*, Journal of Imaging, 2025, 11(2), 58. DOI: <https://doi.org/10.3390/jimaging11020058>
6. Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, 2013.
7. Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach*, Pearson, 2020.
8. Andreas Kaplan & Michael Haenlein (2019), "Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence," *Business Horizons*.

Footnotes:

-
- 1 - Definition provided by ChatGPT (Artificial Intelligence platform), consulted on 05/07/2025..
 - 2 - A. Shchitova, Definition of Artificial Intelligence for Legal Regulation, Proceedings of the 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020), Published by Atlantis Press, pp{616-620}.
 - 3 - Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach*.
 - 4 - Kaplan, A., & Haenlein, M. (2019). "Siri, Siri, in my Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence". *Business Horizons*.
 - 5 - Mohamed Fathy Mohamed Ibrahim, The Legislative Regulation of Artificial Intelligence Applications, *Journal of Legal and Economic Research*, Issue 71, September 2022, p. 1031.
 - 6 - Rabea Ibrahim, The Legal Nature of Artificial Intelligence, *Al-Ustadh Al-Bahith Journal for Legal and Political Studies*, Vol. 10, No. 01, June 2025, p. 537.
 - 7 - *Ibid.*, p. 538.
 - 8 - Russell, Stuart & Norvig, Peter. *Artificial Intelligence: A Modern Approach*. 3rd Edition. Pearson, 2010.
 - 9 - Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*.
 - 10 - **See:** Abdelkader Rahal, *Criminal Protection of the Right to Privacy: A Comparative Study between Islamic Sharia and Algerian Criminal Law*, PhD Dissertation in Islamic Sciences, University of Oran, 2014–2015, p. 38.
 - 11 - **See:** Fadila Berkan, *Protection of the Right to Privacy in Algerian Legislation*, *Algerian Journal of Law and Political Sciences*, Vol. 10, No. 2, 2025, pp. 389–413.
 - 12 - **Abdelkader Rahal**, *ibid.*, p. 40.
 - 13 - Have we ever considered how much personal data we share every day? Whether we are using an application on our phones, browsing social media platforms, or interacting with an intelligent chatbot, a portion of our information is constantly being collected, analyzed, and possibly stored without our awareness. Artificial intelligence has become an integral part of our lives and relies fundamentally on data, which makes the protection of privacy critically important. This protection is no longer an option but a necessity in a digital world where systems compete to know everything about us.
 - 14 - **See:** Ibrahim Riyadh Hegazy Al-Fiqi, The Right to Privacy in the Face of Artificial Intelligence: A Comparative Study between Egyptian Law and European Law, *Ibram Journal of Arts and Human and Social Studies*, Vol. 1, No. 1, Part 7, July 2025, p. 205.

15 - Ibid., p. 206.

16 - Anna Bacciarelli ; "Rights Groups Sound the Alarm on Mass Surveillance Technology" : September 29, 2023 3:09PM EDT. - Anna Bacciarelli ; "Rights Groups Sound the Alarm on Mass Surveillance Technology" : September 29, 2023 3:09PM EDT.

[https://www.hrw.org/news/2023/09/29/time-ban-facial-recognition-public-spaces-and-borders?utm.](https://www.hrw.org/news/2023/09/29/time-ban-facial-recognition-public-spaces-and-borders?utm_source=facebook&utm_medium=share&utm_campaign=facebook) تمت زيارة الموقع الإلكتروني في 2025/11/29

17 - The same article, Human Rights Watch,

<https://www.hrw.org/news/2023/09/29/time-ban-facial-recognition-public-spaces-and-borders>, accessed on 29/11/2025.

18 - The article from *Business Insider* (visited on 24/11/2025) can be cited as:

Business Insider, "Outrage over police brutality has finally convinced Amazon, Microsoft, and IBM to rule out selling facial recognition tech to law enforcement," *Business Insider*, June 2020, <https://www.businessinsider.com/amazon-microsoft-ibm-halt-selling-facial-recognition-to-police-2020-6> (accessed 24/11/2025).

19 - Refer to : Nazar EL Fadel : Facial Recognition Algorithms: A Systematic Literature Review, Journal of Imaging , Department of Computer Engineering, College of Computing, Fahad Bin Sultan University, Tabuk 71454, Saudi Arabia J. Imaging 2025, 11(2), 58; <https://doi.org/10.3390/jimaging11020058> This article belongs to the Section Computer Vision and Pattern Recognition.

20 - Milvus. (2025, November 27). *What are the ethical concerns in predictive analytics*. Retrieved from <https://milvus.io/ai-quick-reference/what-are-the-ethical-concerns-in-predictive-analytics>

21 - Milvus. (2025, November 27). *What are the ethical concerns in predictive analytics?* Retrieved November 27, 2025, from <https://milvus.io/ai-quick-reference/what-are-the-ethical-concerns-in-predictive-analytics>

22 - Rainer Mühlhoff and Hannah Ruschemeierb : Predictive analytics and the collective dimensions of data protection LAW, INNOVATION AND TECHNOLOGY 2024, VOL 16, NO. 1, 261-292 ROUTLEDGE Routledge Taylor & Francis Group Institute for Philosophy & Institute for Cognitive Science, University of Osnabrück, Osnabrück, Germany; Department of Law, University of Hagen, Hagen, Germany. P 262.

23 - Rainer Mühlhoff and Hannah Ruschemeierb : Ibid. p 263.

24 - <https://milvus.io/ai-quick-reference/what-are-the-ethical-concerns-in-predictive-analytics> . 2025/11/28

25 - - Rainer Mühlhoff and Hannah Ruschemeierb, Op. cit, p 263.