



PROTECTION OF THE RIGHT TO PRIVACY FROM THE HARMS OF ARTIFICIAL INTELLIGENCE USE IN ALGERIAN LEGISLATION

P^r .KIHAL Kamal

Ahmed Draia University of Adrar, Algeria

KamelKihel@univ-adrar.edu.dz

Laboratory of Law and Society

D^r. BOULAARES Mokhtar *Echahid Cheikh Larbi Tebessi University,
Tebessa, Algeria

mokhtar.boulaares@univ-tebessa.dz

Laboratory of Law and Society

Send Article Date: 01-06-2025

Date of acceptance of the article: 10-09-2025

Abstract:

There is no doubt that the use of artificial Intelligence has become an integral part of our daily lives, resulting in numerous applications, especially in the field of communication technology and access to Information and personal data. The technological risks associated with AI systems' control over various aspects of society have increased.

These risks have extended to human rights violations, primarily the right Infringement to privacy through attacks on the public data and private institutions and the hacking of Individuals' personal accounts. Thus, the research problem lies in examining the extent to which the Algerian legislator keeps pace with International legal developments to counter the risks of using artificial intelligence on the right to privacy.

Keywords: AI; Privacy; Responsibility; Personal Data.

Introduction:

The uses of artificial intelligence (AI) are witnessing rapid development due to the promising opportunities it offers in various fields. This has driven countries and institutions to work on harnessing its advantages. However, alongside the increasing use of AI, doubts have grown regarding the ability of this technology to protect personal data, given the constant need for AI algorithms to be updated and continuously fed with vast amounts of data and information based on real-life experiences and human interactions with this modern technology.

* BOULAARES Mokhtar.



This leads to AI systems accessing individuals' personal and private data for the purpose of processing and analysis.

Furthermore, instances of unlawful or arbitrary surveillance and interception of communications have increased, along with the collection of personal data in illegal and abusive ways that violate the right to privacy.

In response, the United Nations General Assembly has issued several resolutions on protecting the right to privacy against AI systems, most notably Resolution No 68/167 adopted on 18 December 2013 concerning the right to privacy in the digital age. The resolution affirms that human rights established outside digital systems must be afforded the same protection within these systems (Poscher, R. (2021). pp. 281–289).

As a result, there have been increasing calls to establish clear rules for processing personal data and for data sharing between individuals, various entities, and governments.

States have thus worked to establish legal frameworks to protect personal data from AI technologies.

In this context, the Algerian legislator has sought to align with comparative legislation and follow international trends by enacting a series of legal provisions in this field.

(The Algerian constitutional No. 16-01. Official Gazette No. 14. of 2016) and 2020 (The Algerian constitutional No. 20-442, Official Gazette No. 82. of 2020) emphasized the protection of personal data, following the criminalization of certain offenses infringing on the right to privacy in the amended Penal Code of 2004, as well as the Law on the Prevention and Fight against Crimes Related to Information and Communication Technologies and the Law on the Protection of Natural Persons in the Processing of Personal Data.

Hence, the importance of this study lies in shedding light on the uses of AI and its impacts on human rights, especially the right to privacy, and in clarifying the means of protecting personal data from violations that may result from the use of AI systems.

This raises the following research question:

To what extent are the legal mechanisms established by the Algerian legislator effective in protecting the right to privacy from various violations arising from the use of AI?

To answer this question, we used the descriptive-analytical method in two sections. The first section discusses the impacts of AI on the right to privacy; the second section addresses the legal guarantees for protecting the right to privacy from the risks posed by AI systems.

The first section: discusses the impacts of AI on the right to privacy

Amending and supplementing Law 17/78, established a set of principles related to the collection and analysis of data to ensure integrity.

According to the modern definition, personal data refers to any information relating to a natural person as long as that person is identified or can be identified by any means.

It appears from the foregoing that legal protection of personal data is limited to natural persons, excluding legal entities.

Among the personal data are: name and surname, voice and image, personal numbers, address, marital status, physical characteristics, health status, racial origins, nationality, political opinions, religious beliefs, psychological test results, fingerprints, phone number, vehicle number, bank account, email address, and computer address

First Requirement: Limitations on the Right to Privacy and Judicial Applications

The right to privacy is a cornerstone of human rights, granting individuals control over their personal lives and information. This right, however, isn't absolute; it's subject to limitations imposed by public interest, such as national security or protecting the rights of others, with such restrictions needing to be legally stipulated and necessary. Its judicial applications are evident in safeguarding the sanctity of homes, personal data, and communication secrecy, as well as protecting one's image and the



right to be forgotten online. Courts, strive to balance this right with legitimate interests, imposing penalties on those who violate it.

1. Limitations on the Right to Privacy

The right to privacy cannot be applied without considering other rights that must be taken into account.

Therefore, a balance between rights is necessary by applying the principle of proportionality (Donahoe, & MacDuffee Metzger, 2019, 115–126), which originated in the German constitutional system after World War II and extended to decisions of the European Court of Justice (ECJ) (Raso, F., Hilligoss, Krishnamurthy, Bavitz, & Kim, 2018), which recognizes it as a general principle in law, as well as the European Court of Human Rights (ECTHR), the African Court on Human and Peoples' Rights (ACHPR), and the Inter-American Court of Human Rights (IACTHR) (Villaronga, Kieseberg, & Li, 2018 304–313). It is worth noting that the importance of proportionality becomes evident when there is a conflict between two or more human rights.

The principle of proportionality must be applied to balance conflicting rights. This is achieved through state intervention and its impact on individuals' rights, reflecting the contradiction between collective and individual interests.

In this context, the European Court of Human Rights has followed three criteria to assess the principle of proportionality: suitability, necessity, and the legitimacy of the objective.

Suitability assesses whether the intervention is indeed appropriate to achieve the desired goal; necessity considers whether the measure taken is the least restrictive alternative to the right to privacy, meaning the minimum harm must be inflicted on the right holder; and the legitimacy of the objective requires that the measure restricting the right to privacy be based on domestic national law and aim to achieve a legitimate purpose as stipulated in the restriction clauses of the International

Covenant on Civil and Political Rights or the European Court of Human Rights (Gerke, Minssen, & Cohen, 2020 pp. 295–336).

Thus, proportionality is a balancing mechanism between legal principles of equal value that are simultaneously applicable but conflicting.

It aims to reconcile rights and prioritize one right over another due to the legitimate objectives pursued by the first right.

Among the most important rights of equal value with the right to privacy is the right to information, where the principle of proportionality is applied to reconcile them, as both are constitutional rights.

Accordingly, the exceptions to the right to privacy relate to the right to access certain types of personal data, often relying on artificial intelligence systems, including:

- Personal data related to judicial police reports and preliminary and judicial.
- investigations under judicial supervision;
- Personal information for journalistic purposes or for scientific or historical research purposes;

Personal data processed for obtaining official statistical information or for archiving in the public interest. (Radanliev, 2025, 28–78).

2. Judicial Applications Concerning the Right to Privacy

2.1. The Julian Robinson Case:

2.1.1 Facts:

The Jamaican Parliament enacted the “NIDS” law to provide a system for collecting data on all Jamaican citizens and residents for at least six months. The law required eligible individuals to apply for registration under penalty of criminal conviction, collecting a range of biometric and demographic data and national reference numbers such as taxpayer registration numbers and driver’s licenses to create a national database.

Upon registration, individuals were granted a national ID number as a condition for accessing goods and services from public authorities.



The system allowed access to data without adequate privacy safeguards (Radanliev, 2025, 28–78).

2.1.2 Procedures:

Mr. Julian Robinson, a Jamaican citizen, challenged the constitutionality of certain provisions of the NIDS law, which was enacted on December 8, 2017, claiming it violated the right to privacy guaranteed under the Jamaican Charter of Fundamental Rights and Freedoms of 2011 enshrined in the Jamaican Constitution. The Attorney General argued that the state's intervention under this law was justified to implement the right to privacy because the law aimed at achieving a legitimate objective.

2.2-The Jamaican Supreme Court:

Due to the lack of a pressing need for mandatory registration, the court concluded that the law represented a “disproportionate means of achieving the objective of providing every citizen with reliable identification.” Because it failed to provide adequate safeguards for protecting sensitive information, the Jamaican Supreme Court ruled that the law, in its entirety, was inapplicable.

3. The L.L. v. France Case:

3.1 Facts:

A case was brought by a French citizen seeking divorce. One of the spouses submitted documents concerning the other spouse's health status, which the court relied upon in its ruling.

3.2 Procedures:

The spouse appealed the national court's ruling before the European Court of Human Rights, arguing that the national court's acceptance and reliance on documents related to his health constituted an interference with his right to privacy.

4- The Judgment of the European Court of Human Rights:

The ECTHR held that the fundamental importance of protecting personal data was not proportionate to the aim pursued, and thus was not necessary in a democratic society to protect the rights and freedoms of others.

The court found that the national court's reliance on the medical document was unnecessary to resolve the dispute, as the same result could have been reached without using the document. (Nguyen, Ngo, Hong, & others, 2023, 4221–4241).

Second Requirement: Risks of Artificial Intelligence to the Right to Privacy

The protection of the right to privacy is at the forefront of legal considerations surrounding artificial intelligence. Despite the benefits AI offers to humanity and its service to mankind, it has simultaneously contributed to human rights violations on the open internet, especially the right to privacy, health, education, freedom of movement, freedom of peaceful assembly, freedom of association, and freedom of expression.

1. Risks of Cookies:

Cookies are text files containing packets of information about the websites visited by the user. They help websites recognize the user's computer to provide content faster by storing details like usernames and passwords.

Although some cookies are essential for a website's core functionality, most are used for statistical and marketing purposes, collecting personal data such as user behavior and search history.

These are often shared with third parties like tech companies, social networks, and media platforms. Privacy violation is a key risk of cookies through tracking users and using their information for ads, identity theft, or malicious activities.

Experts argue that cookies themselves are not dangerous, as they are merely text files and not programs or viruses.

However, the risk arises when someone else accesses browser data using hacking techniques to steal cookie content while it is transmitted between the browser and the server.

Governments can also exploit cookies to track users' internet activities by requesting information directly from the server owners. (Gerke, Minssen, & Cohen, 2020, 295–336).



2. Risks of Electronic Surveillance:

With the rise of digital data transmission using AI systems, a national security problem has emerged, facilitating monitoring of individuals, spying on them, and determining their locations. In data transmission, the problem of telecom networks' inability to provide absolute data confidentiality arose, as networks can be exploited to unlawfully obtain personal data remotely. (Felzmann, Fosch-Villaronga, Lutz, & Tamò-Larrieux, 2020, 3333–3361).

3. Risks of Cloud Computing:

Cloud computing refers to computing resources and systems available on demand over the internet, offering integrated computing services without local resource constraints to ease the user's experience.

These resources include data storage, backups, software processing capabilities, and email services.

When connected to the cloud, users can control these resources through a user-friendly interface that hides many internal processes and details.

The risk lies in the fact that once data is used in the cloud, it is transferred and circulated from one place to another over the internet and is subject to smart algorithms that may reveal information the user did not intend to disclose. (Price, W. N., & Cohen, I. G. 2019. 37–43)

4. Risks of Children's Games:

With the widespread use of AI in children's games, the risk of privacy violations has increased through the sharing of children's photos and personal data on social media, including their daily lives and personal details.

These images and videos can be exploited in crimes against children, such as fraud, voice cloning, sexual abuse, and abduction. UN reports indicate that around 80% of children in 25 countries have faced risks of sexual abuse and exploitation online. Risks include online harassment, cyberbullying, hacking,

deepfakes, and cyber extortion (Felzmann, , Fosch-Villaronga, Lutz, & Tamò-Larrieux 2020 3333–3361).

5. Risks of AI to Health Privacy:

AI became particularly significant during the Covid-19 pandemic by tracking and tracing cases to combat the virus. However, legal, ethical, and health concerns emerged regarding its use in tracking individuals' health status.

The World Health Organization warned that health privacy faces cybersecurity risks, potentially jeopardizing patient information and the reliability of healthcare services."

Section Two: Legal Guarantees to Protect the Right to Privacy from the Risks of Artificial Intelligence Systems

In recent years, there has been a noticeable legislative development through the adoption of numerous legal and regulatory texts related to communication technologies, establishing certain rules aimed at protecting user privacy.

These legislative developments in Algeria are part of an effort to align with international conventions and comparative legislation in this field, starting with the Penal Code, particularly the amendment of 2004, the law on special rules for the prevention and fight against crimes related to information and communication technologies, the media law, and finally, the law on the protection of personal data (First Requirement). With the evolution of daily practices that violate the right to privacy, the Algerian legislator has also established some procedural rules in various texts to enhance the legal protection of personal data (Second Requirement).

First Requirement: Substantive Rules to Protect the Right to Privacy from the Harms of Artificial Intelligence

The recent legislative developments in Algeria, through the enactment of several laws related to communication technologies, have attempted to establish certain rules aimed at protecting user privacy.



However, most of these attempts remain insufficient in addressing the risks posed by AI systems. We will focus on the main legislative attempts in this field as follows:

1- Law No. 04-15 Related to the Penal Code

Through the amendment of the Penal Code in 2004 Algeria. (2004). (Penal Code Law No. 04-15., Official Gazette N 71 of 2004) the Algerian legislator reinforced the protection of the right to privacy by criminalizing certain acts, notably offenses against automated data processing systems, including unauthorized access and presence in an information system, and the destruction of automated systems through specific means, such as computer viruses.

1-1- The Crime of Fraudulent Access to an Automated System

Article 394 bis states: “Shall be punished by imprisonment from three months to one year and a fine from 50,000 DZD to 100,000 DZD anyone who fraudulently accesses all or part of an automated data processing system.”

The material element of the offense consists of unauthorized access to all or part of the system by any person, with the intent and deliberate nature of the act being essential, as it is considered an intentional crime. There must also be specific criminal intent, namely fraud.

1-2- The Crime of Unauthorized Stay in an Information System

Article 394 bis also covers: “...or remains fraudulently in all or part of an automated data processing system...” The offense is constituted by remaining in the system against the will of the person entitled to control it.

This misdemeanor is punishable independently of the crime of fraudulent access. Both offenses can occur together when the perpetrator unlawfully enters the system and then remains within it.

This crime is considered continuous, lasting as long as the unauthorized presence continues. It does not require intent to

harm the system; mere unauthorized stay suffices. Penalties range from 3 to 6 months of imprisonment and fines from 50,000 to 1,000,000 DZD.

2- The Crime of Destroying an Automated Data Processing System

This offense involves damaging computer programs or data, or deleting program instructions and data themselves.

The legislator referred to destruction using terms such as (inserted; removed; modified), all falling under the concept of destruction, which can be achieved by any means, most notably through computer viruses self-replicating and spreading programs designed to move from system to system, often hidden within legitimate software, and intended to destroy other programs.

This is an intentional crime requiring the general criminal intent that the perpetrator is aware that the property damaged belongs to others and that the act would destroy, disable, or devalue it. (Ben Massoud, 2017, 487–500).

3- Law No 09-04 on Special Rules for the Prevention and Fight Against Crimes Related to Information and Communication Technologies

As part of efforts to protect personal and public data, the legislator enacted Law No. 09-04, (the prevention and fight against crimes related to information and communication technologies Law No. 09-04 Official Gazette No. 47 of 2009) classified within AI systems according to Article 1. Article 2 defines key concepts for protecting privacy and public data:

3-1- Crimes Related to ICT

These include offenses against automated data processing systems defined in the Penal Code and any other crime committed or facilitated through an information system or electronic communications network.



3-2- Information System

Any standalone system or interconnected group of systems that perform automated data processing based on a specific program.

3-3- Data

Any presentation of facts, information, or concepts in a form ready for processing within an information system, including relevant software enabling the system to perform its function.

3-4- Service Providers

Any public or private entity providing users with access to communication via an information system or communication network.

Any entity processing or storing data for the mentioned communication service or its users.

3-5- Traffic Data

Data related to communication via an information system generated by the system as part of the communication process, indicating the source, destination, route, date, time, duration, volume, and type of service.

3-6- Electronic Communications

Any transmission, sending, or receiving of signals, writings, images, sounds, or various information by any electronic means.

4- Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data

Law No. 18-07 establishes a set of rights for data subjects to ensure lawful use of their personal data, mainly: (the protection of individuals in the processing of personal data Law No. 07/2018. Official Gazette No. 34.of 2018).

4-1- The Right to Prior Information about the Identity of the Processing Controller

The law requires the entity responsible for processing to inform the data subject in advance and obtain consent, except in cases such as processing for statistical, historical, or scientific purposes, or when mandated by law or for journalistic purposes.

4-2- The Right of Access

The individual has the right to inquire and verify whether their personal data is being processed.

4-3- The Right to Rectification

Individuals can request to amend, correct, erase, or block data processed unlawfully.

4-4- The Right to Object

Any person whose data is unlawfully processed can object to the processing. They may also object if their data is used for advertising or commercial purposes unless the processing is legally mandated (e.g., by court order or with consent).

4-5- Ban on Direct Prospecting

The legislator prohibits direct prospecting via communication systems, remote copying devices, or email without the data subject's consent.

Additionally, the law imposes several obligations on the data processing controller (Articles 38 to 45 of Law 18-07), such as:

Ensuring confidentiality and integrity of processing by implementing appropriate technical, organizational, and security measures to protect data from damage, disclosure, or unauthorized access.

Maintaining confidentiality of data encountered during processing and ensuring data security, whether processed directly or through subcontractors like internet service providers.

Handling personal data related to electronic certification and signature services, ensuring that only concerned persons can access and process relevant documents after obtaining consent.

Prohibiting the transfer of personal data to foreign countries without authorization from the national authority and consent from the data subject.



Second Requirement: Procedural Rules for Protecting the Right to Privacy from the Harms of Artificial Intelligence

The legislator has established an institutional framework to enforce procedural protection of the right to privacy in the digital age, which relies on artificial intelligence, as follows:

1- The National Body for the Prevention and Fight Against Crimes Related to Information and Communication Technologies

This body is responsible for activating and coordinating the prevention of crimes related to information and communication technologies and fighting them.

It assists judicial authorities and law enforcement in investigations concerning crimes related to information and communication technologies, including gathering information and conducting judicial expertise.

It exchanges information with its counterparts abroad to collect all useful data to identify and locate perpetrators of crimes related to information and communication technologies.

2- The National Authority for the Protection of Personal Data

The Algerian legislator ensured procedural protection of personal data by establishing the National Authority for the Protection of Personal Data under the provisions of Law No. 18-07. This authority oversees respect for human dignity and the right to privacy during the processing of personal data; grants permits; and receives declarations related to the processing of personal data.

In addition to its remedial role, it informs data subjects of their rights, which include the right to be informed, the right of access, the right of rectification, the right to object, and the prevention of direct marketing.

It also informs data controllers of their obligations, including confidentiality and data processing integrity. The national authority also has procedural duties, such as inspecting premises and locations where data processing occurs; accessing processed data; and collecting information and

documents. (Appointing the President and members of the National Authority for the Protection of Personal Data Decree No. 22-187, Official Gazette No. 35 of 2022).

3- The National Council for the Security of Information Systems

The misuse of information and communication technologies, the rise of computer-related crimes, and technological crimes involving artificial intelligence systems have led legal systems to establish bodies concerned with cybersecurity to combat cyber threats, especially service disruption, data destruction or alteration, espionage on networks, and destruction of assets and information. (Defining the tasks of the Executive Secretariat of the National Authority for the Protection of Personal Data Presidential Decree No. 23-73 Official Gazette No. 10 of 2023). In this context, Algeria has aimed to implement a comprehensive strategy. Presidential Decree No. 20-05 was issued to establish a national system for the security of information systems.

The Algerian legislator introduced mechanisms under the supervision of the Ministry of National Defense, as cybersecurity issues relate to the sovereignty of the Algerian state (Establishing a national system for information system security. Presidential Decree No. 20-05 Official Gazette No. 4. of 2020). According to Article 3 of the decree, "the national system for the security of information systems established under the Ministry of National Defense includes:

A National Council for the Security of Information Systems, referred to in the text as 'the Council,' responsible for preparing the national strategy for the security of information systems;

An agency referred to in the text as 'the Agency,' responsible for coordinating the implementation of the national strategy for the security of information systems."

The National Council for the Security of Information Systems is tasked with preparing a national strategy for information systems security, reviewing and approving reports on the implementation of the national strategy, approving the electronic certification



policy of the National Authority for Electronic Certification, approving the classification of information systems, and proposing adjustments to the structural or organizational framework related to information systems security.

Conclusion

International legal systems have tried to establish a legal framework to protect personal data from the misuse of artificial intelligence systems and their risks, especially the hacking of personal electronic communications, unauthorized access to data, and remaining unlawfully without legal grounds.

The Algerian legislator has worked to establish a legal framework to protect the right to privacy from the harms of artificial intelligence. From the study, the following findings and recommendations have been reached:

A- Results

The uses of artificial intelligence have evolved to encompass all areas of life, including human privacy.

The Algerian legislator has tried to establish an institutional framework to ensure necessary protection of the right to privacy from various infringements, particularly the risks of artificial intelligence.

Preventive protection of the right to privacy from the risks of artificial intelligence is still lacking, as the Algerian legislator lags behind comparative legislations in establishing a protective legal framework, despite positive efforts. This is mainly due to the novelty of the right to privacy and artificial intelligence in Algerian legislation.

There is no balance between the requirements of protecting the right to privacy on the one hand and the right to access information through artificial intelligence techniques on the other.

There is no effective legal framework defining the regulations for using artificial intelligence or rules for civil liability for its risks, especially concerning the right to privacy.

B/ Recommendations:

Draw clear guidelines that balance the fundamental human right to privacy and the right to access information via artificial intelligence techniques.

The Algerian legislator should establish a legal framework to amend civil liability rules to address the harms of artificial intelligence systems.

Enact legal provisions that include preventive systems to compensate for damages resulting from artificial intelligence technologies, especially those affecting the right to privacy.

Establish the principle of transparency in disclosing the methods used by artificial intelligence technologies and inform citizens about the imposition of these technologies and how they are employed.

Ensure the proper use of individuals' personal data and protect it from any exploitation or violation of private life.

List of References**1- Laws**

- Algeria. (2004). Law No. 04-15 of November 10, 2004, amending and supplementing Ordinance No. 66-156 on the Penal Code. Official Gazette No. 84. <https://www.joradp.dz/FTP/jo-abe/2006/A2006084.pdf>
- Algeria. (2009). Law No. 09-05 of August 5, 2009, on the prevention and fight against crimes related to information and communication technologies. Official Gazette No. 47 of 2009. <https://www.arpce.dz/ar/pub/19d1a8>
- Algeria. (2016). Law No. 16-01 of March 6, 2016, amending the Constitution. Official Gazette No. 14. <https://www.joradp.dz/FTP/jo-arabe/2016/A2016014.pdf>
- Algeria. (2018). Law No. 18-07 of June 10, 2018, on the protection of individuals in the processing of personal data. Official Gazette No. 34. <https://www.arpce.dz/ar/pub/c7e6n6>
- Algeria. (2020). Presidential Decree No. 20-05 of January 20, 2020, establishing a national system for information system security. Official Gazette No. 4. <https://www.arpce.dz/ar/pub/i0h6b2>
- Algeria. (2020). Presidential Decree No. 20-442 of December 30, 2020, on the new Constitution. Official Gazette No. 82.



- <https://www.joradp.dz/TRV/A2022B14.pdf>
- Algeria. (2022). Presidential Decree No. 22-187 of May 18, 2022, appointing the President and members of the National Authority for the Protection of Personal Data. Official Gazette No. 35.
- <https://www.joradp.dz/FTP/jo-arabe/2022/A2022035.pdf>
- Algeria. (2023). Presidential Decree No. 23-73 of February 14, 2023, defining the tasks of the Executive Secretariat of the National Authority for the Protection of Personal Data. Official Gazette No. 10. <https://www.joradp.dz/FTP/jo-arabe/2023/A2023010.pdf>

2- Articles

- Ben Massoud, A. (2017). Crimes against automated data processing systems in Algerian legislation. *Journal of Law and Political Science*, 10(1), 487–500. <https://asjp.cerist.dz/en/article/18306>
- Donahoe, E., & MacDuffee Metzger, M. (2019). Artificial intelligence and human rights. *Journal of Democracy*, 30(2), 115–126. <https://doi.org/10.1353/jod.2019.0029>
- Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2020). Towards transparency by design for artificial intelligence. *Science and Engineering Ethics*, 26, 3333–3361. <https://doi.org/10.1007/s11948-020-00276-4>
- Gerke, S., Minssen, T., & Cohen, I. G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In E. R. Shortliffe & J. J. Cimino (Eds.), *Artificial Intelligence in Healthcare* (pp. 295–336). Academic Press. <https://doi.org/10.1016/B978-0-12-818438-7.00012-5>
- <https://doi.org/10.1017/9781009207898.022>
- Nguyen, A., Ngo, H. N., Hong, Y., & others. (2023). Ethical principles for artificial intelligence in education. *Education and Information Technologies*, 28, 4221–4241. <https://doi.org/10.1007/s10639-022-11316>
- Poscher, R. (2021). Artificial intelligence and the right to data protection. In C. Docksey, E. Kosta, & I. G. Cohen (Eds.), *Data Protection and Privacy: The Internet of Bodies* (pp. 281–289). Cambridge University Press.
- Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature Medicine*, 25, 37–43. <https://doi.org/10.1038/s41591-018-0272-7>
- Radanliev, P. (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains,

and quantum computing. *Journal of Cyber Security Technology*, 9(1), 28–78. <https://doi.org/10.1080/23742917.2024.2312671>

- Raso, F., Hilligoss, H., Krishnamurthy, V., Bavitz, C., & Kim, L. Y. (2018). Artificial intelligence & human rights: Opportunities & risks. Berkman Klein Center Research Publication No. 2018-6. <https://ssrn.com/abstract=3259344>
- Villaronga, E. F., Kieseberg, P., & Li, T. (2018). Humans forget, machines remember: Artificial intelligence and the right to be forgotten. *Computer Law & Security Review*, 34(2), 304–313. <https://doi.org/10.1016/j.clsr.2017.08.007>