

**Digitalization and International Human Rights Law: the Protection of
the Right to Digital Privacy in the AI Era[#]
Hamzah Suleiman Aldoghmi^{(1)*}**

(1) Researcher, Faculty of Law, Al-alBayt University, Jordan.

Received: 1/2/2026

Accepted: 10/5/2026

Published: 23/7/2026

*** Corresponding Author:**

DOI:
<https://doi.org/10.59759/law.v5i2.1972>

Abstract

Digital privacy rights in the age of artificial intelligence (AI) have become the critical component of data safety and privacy rights within the modern digital environment. With the rapid adoption of AI technologies in a variety of aspects of everyday experience, the issue of the security and privacy of personal data has increased. People should be able to control their information and they should be guaranteed that their data will not be escaped or misused. This is especially needed because the AI systems are becoming skilled in harvesting, analyzing, and consuming large

amounts of personal information. The developers and firms working in the field of AI ought to pay more attention to privacy using the strongest encryption tools, safe storage measures, and clear guidelines on data-processing. In addition, laws should advocate this right by making organizations responsible whenever their activities were violated or abuse of the rights of digital privacy. In protecting the right to online privacy in AI, it is essential to maintain trust in new technologies and prevent individuals by being harmed or abused in some way. The problem of AI and digital privacy has become more and more obvious. The right of people to their digital privacy is more than ever since the advent of AI

[#] A special issue for the Third International Conference, entitled: **Artificial Intelligence, A Legal Vision Towards a Sustainable Future**.

technology and its integration into many spheres of life. Digital privacy is a basic human right, and it should be ensured and preserved during the production and implementation of AI technologies. In line with this finding, the present study will provide an in-depth analysis of the intersection of digital transformation with the international human rights law, specifically the law of the right to digital privacy in the era of artificial intelligence. The research, based on the descriptive and analytical approach, outlines the right to digital privacy and examines the law that is relevant to its protection in the era of the digital revolution in the age of artificial intelligence. The paper argues that there will be no safeguarding of privacy and personal data unless domestic law is enacted that provides protections over individual personal data and an electronically aware society that will increase the awareness of any potential dangers of technology effects on privacy. Moreover, it is necessary that states join forces towards protecting the right to digital privacy and address cybercrime and privacy violations.

Keywords: Digitalization, The Right to Digital Privacy, Artificial Intelligence, International Human Rights Law.

الرقمنة والقانون الدولي لحقوق الإنسان، حماية الحق في الخصوصية الرقمية

في عصر الذكاء الاصطناعي

حمزة سليمان الدغمي⁽¹⁾

(1) باحث، كلية الحقوق، جامعة آل البيت، الأردن.

ملخص

أصبحت حقوق الخصوصية الرقمية في عصر الذكاء الاصطناعي عنصراً أساسياً في أمن البيانات وحقوق الخصوصية ضمن البيئة الرقمية الحديثة. ومع الانتشار السريع لتقنيات الذكاء الاصطناعي في مختلف جوانب الحياة اليومية، تزايدت أهمية أمن البيانات الشخصية وخصوصيتها. حيث ينبغي أن يكون للأفراد الحق في التحكم بمعلوماتهم، وأن تُضمن لهم حماية

بياناتهم من التسريب أو سوء الاستخدام. وتزداد هذه الحاجة إلحاحاً مع تطور أنظمة الذكاء الاصطناعي وقدرتها على جمع وتحليل واستخدام كميات هائلة من المعلومات الشخصية. لذلك يجب على المطورين والشركات العاملة في مجال الذكاء الاصطناعي إيلاء مزيد من الاهتمام للخصوصية، باستخدام أقوى أدوات التشفير، وتدابير التخزين الآمنة، ووضع إرشادات واضحة لمعالجة البيانات. إضافةً إلى ذلك، ينبغي أن تدعم القوانين هذا الحق، وأن تُحمّل المؤسسات المسؤولية في حال انتهاكها لحقوق الخصوصية الرقمية أو إساءة استخدامها. ولحماية الحق في الخصوصية على الإنترنت في ظل الذكاء الاصطناعي، من الضروري الحفاظ على الثقة في التقنيات الجديدة، وحماية الأفراد من أي ضرر أو إساءة استخدام. لقد باتت مشكلة الذكاء الاصطناعي والخصوصية الرقمية أكثر وضوحاً من أي وقت مضى. أصبح حق الأفراد في الخصوصية الرقمية أكثر أهمية من أي وقت مضى منذ ظهور تقنيات الذكاء الاصطناعي ودمجها في مختلف مجالات الحياة. فالخصوصية الرقمية حق أساسي من حقوق الإنسان، ويجب ضمانها والحفاظ عليها أثناء إنتاج وتطبيق تقنيات الذكاء الاصطناعي. وانطلاقاً من هذا، تُقدم هذه الدراسة تحليلاً معمقاً لتداخل التحول الرقمي مع القانون الدولي لحقوق الإنسان، وتحديدًا قانون الحق في الخصوصية الرقمية في عصر الذكاء الاصطناعي. ويستند البحث، الذي يعتمد على المنهج الوصفي والتحليلي، إلى تحديد الحق في الخصوصية الرقمية ودراسة القوانين ذات الصلة بحمايته في عصر الثورة الرقمية والذكاء الاصطناعي. وتؤكد الدراسة أنه لن يكون هناك حماية للخصوصية والبيانات الشخصية ما لم يتم سن قوانين محلية توفر الحماية للبيانات الشخصية للأفراد، ومجتمع واعٍ إلكترونيًا يزيد من الوعي بالمخاطر المحتملة لتأثيرات التكنولوجيا على الخصوصية. علاوة على ذلك، من الضروري أن تتضافر جهود الدول لحماية الحق في الخصوصية الرقمية والتصدي للجرائم الإلكترونية وانتهاكات الخصوصية.

الكلمات المفتاحية: الرقمنة، الحق في الخصوصية الرقمية، الذكاء الاصطناعي، القانون الدولي لحقوق الإنسان.

1. Introduction

The digitalization of society has made such a connection and access to information unmatched, thus changing communication, work and everyday living. However, this shift to a digital milieu is at the same time raising some fundamental questions related to the protection of human rights in the digital space. With an ever-growing fraction of all the activities in our

daily lives being mediated by the online platforms, it is imperative to carefully explore the impact of digitalization on the key human rights, i.e., privacy, freedom of expression, and access to information.

At the point of digitalization and human rights, the issue of privacy is one of the major concerns. The en masse use of social media, mobile devices and internet based service has created endless generation of bulk personal information, easily accessible to be collected, stored, and analyzed by corporations and government agencies. A body of academic studies has been released in an attempt to reduce the state abuse of individual data, thus enhancing the necessity of protecting the right to privacy and confidentiality of personal information in the digital era.¹ This has led to the need to create a working relationship between the government and technology companies that will help in the development of clear rules and regulatory standards that will strengthen the privacy rights of individuals in the cyber world.

Digitalization has its control on the freedom of expression alongside the privacy issue. Although the internet allows people to find new opportunities to express themselves and get access to a wide range of informational resources, it also encourages the spread of hate speech, misinformation, and harassment via the internet.² In such a way, it is the responsibility of the systems to curb undesirable online material, which should be properly balanced with the maintenance of free expression. The internet is a platform of information dissemination and storage of collective knowledge in various fields of society. Therefore, it is the duty of government institutions and information technology corporations to come up with collaborative measures. These measures can adequately curb online abuse and provide a safe and inclusive online environment to users.

Moreover, the phenomenon of digitalization has the ability to enrich or hinder the informational availability and learning of knowledge. Even though the internet has led to a democratization of the availability of information in many aspects, there are still long lasting barriers connected

¹ Younes Arab, The Role of Privacy Protection in Creating Change in Society, Digital Blog in the Symposium of the Arab Information Ethics Club, October 17-18, 2002, Amman, Jordan, p. 7.

² Nahla Al-Momani, Cybercrimes, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2008, p. 38.

to digital literacy and connectivity that marginalizes groups of the population, thus preventing full involvement in the digital age. This forces governments and policy makers to focus on initiatives that will help in closing the digital divide and enabling equal opportunities to all people in the digital ecosystem to participate and contribute.

Human rights protection presents opportunities and challenges in a society that is becoming digitalized. An integrated effort between governments, information technology institutions, and the civil sector has become a prerequisite in protecting the basic human rights of people in the digital realm as the new issues are negotiated. It can be seen that through the establishment of coherent regulatory frameworks, the promotion of digital literacy, and the fight against online mischief, it can be made possible to guarantee that digital transformation can benefit everyone, maintain, and preserve the fundamental human rights.

Artificial intelligence (AI) is now an inseparable part of everyday life, which includes virtual assistants, self-driving cars, and drones. Although AI has enormous potential to enrich many aspects of human life, it also, conversely, leads to the creation of fears of what their human rights violations might be. The nexus between AI and human rights is a topical problem given the implication and challenges presented by this rapidly growing field.

One of the exigent issues that have been raised concerning AI and human rights is the likelihood of discrimination and algorithmic bias in AI. Such systems get trained using high volumes of data and bias in such a data can result in biased results. As an example, AI algorithms applied in the criminal justice realm may exhibit racial bias in predicting a recidivism, which in turn promotes prejudiced treatment of disadvantaged groups of people. In order to prevent such bias and protect human rights, AI systems should be transparent, accountable, and have clear decision-making policies.

The other notable source of concern relates to the aspect of AI and privacy and security. Surveillance systems based on AI can violate the right of individuals to their privacy, and the consequences of implementing AI will have extensive effects on the freedom of speech and association. Therefore, law enforcement and business leaders should create a wise balance between the application of AI in the security sphere and the right to privacy of citizens. There is no room to ignore strong regulations and

protection, which is essential to avoid the exploitation of AI technologies and to preserve human rights.

Besides, AI provokes significant anxieties about job opportunities and the associated rights of workers. With the development of AI, there are high chances of massive labor replacement and the consequent economic inequality. It is therefore crucial to address how AI will affect the rights of the workers such as employment security, fair pay, or training and education opportunities. Governments and companies should invest in strategies and programs that will not leave workers behind during the automation process.

Besides, the development of AI-controlled weapons and autonomous systems is raising serious ethical considerations in the framework of the international human rights and humanitarian law. The AI-enabled weapons have the ability to identify and attack targets independently, thus, posing essential inquiries of responsibility and safety of the civilians during a military conflict. Policymakers and ethicists should therefore address such dilemmas and establish rule making that will provide the responsible use of AI in military and security application within the internationally accepted human rights standards.

The incorporation of AI in the social systems has two possible opportunities and creates challenges in relation to human rights. To protect the human dignity and rights, it is necessary to consider the ethical implications of AI, such as discrimination, encroachment of privacy, labour market changes, and military use. Promoting transparency, accountability, and human-rights-oriented principles in the process of AI design and implementation, the advantages of AI can be enjoyed and at the same time avoid infringing upon the dignity and rights of every member of the society that is becoming digitalized with each passing day.

Accordingly, this paper predicts the effects of digital transformation on legal protection of the right of digital privacy. It does so by evaluating the interaction between digitalization and AI technologies. It discusses how such interrelations interact with the safeguards provided by the international human-rights law to the right of digital privacy in a rapidly changing environment. This requires defining the protection required by the international jurisprudence to safeguard personal information and ensure individual privacy.

1.1 Research Problem

The research problem is the suitability of the protection of the right to privacy afforded by the international human rights law especially against the backdrop of scientific and technological advancements, in the digital age as well as the modern world of the technology of artificial intelligence.

1.2 Research Questions

Referring to the research problem outlined in this introduction, the following major question will be answered in this research study:

Does the international human rights law provide protection to the right to digital privacy in the era of artificial intelligence?

In order to respond to this major question, the following subsidiary questions are developed:

- What is digital transformation?
- What is the artificial intelligence technology?
- What effect does artificial intelligence have on the right to digital privacy?
- What are the legal provisions protecting the right to privacy in digital form?

1.3 Research Methodology

The research follows a mixed-method design, that is, it utilizes descriptive and analytical research. The scientific and technological reasons that affect the right to digital privacy are outlined first, and the legal guarantees that are provided by the international human rights law are examined. The study, then, evaluates how modern technologies, i.e. digital transformation and artificial intelligence, impact the right to privacy, and considers the relevant legal protection of the right to privacy that ensues the impact.

1.4 Existing Literature

Abeer Al-Obaidi, The Human right to privacy under the conditions of the digital revolution, Journal of Jurisprudential and Legal Research, Al-Azhar University, Issue 44, January 2024, (1057-1134).

This paper explores breaches of the right to privacy created by scientific and technological innovations linked to the digital revolution, the conflict between the human right to privacy and the needs of digital surveillance, and the international legal standards that govern the privacy protection.

Nahla Al- Warfali, *The Right to Privacy in the Digital Age, Al-Haq Journal of Sharia and Legal Sciences, Bani Walid University, Issue 14, December 2024, (139 -157).

This paper discusses the meaning of information privacy, assessment of information privacy jeopardies, and discussion of legal safeguards. It also examines what can be done to ensure the privacy right is respected and how a legislative intervention is desirable to protect the privacy, by providing criminal sanctions to digital privacy breaches and maintain the privacy of the lives of individuals.

Ahmed Iman, The Necessity of Protecting Human Rights in the Digital Age, Al-Ustadh Al-Bahith Journal of Legal and Political Studies, Vol. 7, October 2022, (470-483).

This paper presents the definition of digital rights, types, and features, the problem of infringement of the right to digital privacy and the discussion of international efforts to uphold the right to digital privacy.

Aisha Bin Qara Mustafa, The Right to Information Privacy: Between Technological Challenges and the Reality of Legal Protection, Arab Journal of Science and Research, Volume 2, Issue (5) June 2016, (38 -52).

This paper examines national, regional and international campaigns to defend the human right to privacy, analyzes the impact of information technology on the right, singles out technical issues associated with personal data, and reviews legal measures that are aimed at protecting personal data and the human right to privacy.

2. Digital Transformation and Artificial Intelligence Technology

Digitalization and artificial intelligence are fast-growing fields that are completely changing the way businesses are being conducted plus how people deal with technology in society. Digitalization refers to the systematic transformation of information into electronic forms which therefore helps in the storage, retrieval and processing of information. With the digital infrastructures creeping into various industries, the amount of data being generated is growing exponentially thus requiring sophisticated analytics tools and technologies that are capable of controlling and interpreting large volumes of data, which has led to the birth of artificial intelligence.

Artificial intelligence is a subfield of computer science that is dedicated to the creation of systems that imitate human mental processes- visual perception, speech recognition, decision-making, and linguistic translation. Machine learning and deep learning are some of the technologies, which enable computational devices to learn through data, detect patterns and

make predictions without procedural programming. As a result, new avenues are created in which businesses can automate operations, improve customer relationships, and derive insights on data that remained hard to reach using traditional analysis techniques.

However, even national legislation and international legal frameworks have not yet kept up with the pace of the rapid growth of digital transformation and artificial intelligence. As a result, states have turned to non-legislative tools, such as policy instruments and administrative decree, to control technological advancement in the process of digitalization and AI. An important example of this situation could be seen in European states, where the governmental actions have urged the private sector to take up the codes of conduct that protect personal data in the context of the global communications, which has secured a privacy-saving network.¹

Digitalization and artificial intelligence are converging to transform almost every sphere of life, healthcare, finance, manufacturing, and transport. Companies currently use data analytics with AI capabilities to optimize their processes, personalize customer experiences, and gain a competitive edge in the market. But the rapid development of AI technologies has led to ethical and cultural issues, including unemployment, data privacy, or algorithm prejudice. With the spread of the use of digitalization and AI, it is necessary to discuss these issues to provide the responsible use that would benefit the common good of society. In line with this, this section will discuss the digital and AI technologies in two separate parts as follows.

2.1 Digital Technology

In the modern setting, digitalization has radically changed the management of corporations and the general interaction with technology. This is a radical process that has entailed the incorporation of digital tools in the various fields of society, which has led to increased productivity, connectivity, and creativity. Digitalization has reshaped economies and industries across the world, starting with the use of big-data analytics through to the use of artificial intelligence. Business organizations and individuals who are operating in the digital era need to understand the

¹ Fawzi Oussedik, The Problem of Information Technology between the Right to Privacy and Disclosure of Professional Secrets, Journal of Legal Studies, Al-Basira Center for Educational Research and Consulting, Issue Two, September 2008, Algeria, p. 77.

underlying principles, technological backgrounds, and implications of digitalization.

The last few years have seen the digitalization becoming a ubiquitous phenomenon that has changed the way information and communication are processed, disseminated and transmitted. The recent high pace of technology changes has enabled digital transformation in many sectors such as the public administration, commerce, education, and health sector. The term digitalization can be defined as the introduction of digital technologies in all spheres of human activity in order to improve its productivity, efficiency in communication, and efficacy of operations.

The main benefits of digitalization are that it is much easier to access, store, and spread information. The use of modern digital gadgets, computers, tablets, smart phones, allows communication between the geography without delays and thus, eliminates the limitations previously present and promotes integration of the world. Additionally, digitalization has simplified a lot of activities hence increasing productivity and efficiency in personal and professional life.

The digital banking and e-commerce platforms have, as an example, significantly decreased the temporal and effort requirements linked to financial operations. Digitalization has also provided immense advantages to organizations in that they can reach more people and optimize their operations. Removing the need to maintain paper records, businesses are able to gather and process large volumes of data in real-time by digitalizing their processes, as such that they can respond quickly to changes in the market and make informed decisions. As a result of this, the competition has become even more intense and the business success is becoming more reliant on agility and adaptability. Additionally, the differentiated customer experience is made possible by targeted marketing campaigns and personalized products and services that are made possible by digitalization. This leads to increased revenue growth and sustainable development as there is increased customer satisfaction and loyalty.

Digitalization has transformed the learning and teaching process in the education sector. Online learning has opened more opportunities to education, decreasing the obstacles to university admissions and encouraging life long learning. Students are now able to access educational materials and communicate with teachers all over the globe hence broadening intellectual boundaries and capability development. Also,

digitalization has released new forms of pedagogy, including gamified learning and more immersive virtual reality experiences, that are not only engaging to students but also enhance the learning outcomes.

Along with its numerous advantages, digitalization has ethical problems that require a thorough approach. The growing reliance on digital technologies provokes doubts about the privacy of data, their safety, and the possibility of social isolation and technological addiction. Additionally, there is an increasing digital divide that is pitting the people who have access to digital resources and those who lack them, hence increasing the society inequities. There is a need to ensure that digitalization can be beneficial to all the members of the society by collaboration between policymakers, businesses, and individuals to facilitate equality and inclusion.

Digitalization is one of the revolutionary powers that is changing the way we live, work and interact. The potential of its effects on people, organizations, and society overall is tremendous, which allows unprecedented innovation, cooperation, and development. Through responsible and ethical use of digital technologies, it is possible to create a more connected and successful future of further generations. Nonetheless, this vision would have to rely on legal framework, which would have international human rights law provisions to protect the rights, which are subject to this scientific and technological development.

2.2 Artificial Intelligence Technology

Artificial intelligence, or AI, is a fast-growing scientific field that has considerable potential to make many industries change. Don't automatically turn off the computer-controlled car or switch off the TV to watch TV programs? AI is already a part of daily life, and it might be even unnoticed at a glance.

Artificial intelligence (AI) has become an indispensable part of people. The new strides in machine learning and deep-learning algorithms make AI capable of performing tasks that are normally demanding human thought. The technology is able to decode and examine large masses of data in a much more rapid and precise way than humans can, and therefore has enormous effects in healthcare, banking and transportation.

One of the main advantages of the AI technology is its ability to analyze and process data. Using algorithms, neural networks, the AI systems are able to identify trends, tendencies, and correlation within large amounts of

data that would normally be difficult to review by humans, which provides the organizations with useful information that informs the making of decisions and helps to improve the efficiency in general.

Besides, AI has the capacity of transforming the healthcare industry by early detection and diagnosis of diseases. AI-based machine-learning algorithms can be trained to analyze medical images and patient records, providing more accurate and faster diagnosis; moreover, artificial intelligence-enhanced robotic surgery can help surgeons to perform more sophisticated procedures more accurately.

Finance Artificial intelligence is commonly used in finance to predict market trends and optimize trading schemes. Through historical and real-time market analysis, AI systems can make more informed investment decisions, which can more likely bring greater returns to the investors. Moreover, banking institutions are also using AI-driven chatbots to provide individualized customer care and assistance.

In the transport industry, AI leads to innovations in the field of autonomous vehicles. AI algorithms allow self-driving cars to drive through the roads, identify impediments, and take quick decisions to keep the travel safe and efficient, which is also capable of fundamentally changing the mobility trends and significantly decreasing accidents on the highway.

Artificial intelligence has the potential to change various industries and significantly improve the quality of life. Constant advances in AI present immense social values, but it is important to comprehend the ethical impact of AI and regulate its safe and ethical usage.

AI has changed how people live, work, and respond to the surrounding environment. Since the deployment of virtual assistants to the driving of autonomous vehicles, the AI has infiltrated various aspects of our existence, and as much as the technology is beneficial to a wide range of industries, it brings about a range of ethical issues, future trends, and potential challenges, which require the creation of regulatory frameworks to control its widespread adoption.

3. Protecting the Right to Digital Privacy

The right to privacy is an inherent human right covered by numerous international treaties and conventions.¹ The right to privacy in the modern digital age has taken different purposes due to the increased pace of technological development. Digital privacy entitles allow individuals to possess the means of controlling their personal details and internet actions, including the possibility to protect personal information against the presence of third parties, any spying attempts, and manipulation of this information by the government and corporations, among others.

Another strong reason in support of the right to privacy in the digital world is the fact that personal data of people should be protected against misuse or abuse. Living in the globalized world, individuals exchange personal information in the social media, e-commerce, and other online services and governments and companies can use this information to spy on them or conduct targeted advertising or any other activity without their approval, which makes it important that strong regulatory measures exist.

In addition, the freedom of expression on the internet cannot be secured without the right to digital privacy. In the age of widespread censorship and monitoring, people need to have the ability to communicate and express themselves openly without fear of punishment and surveillance so that the digital realm would not become a place of suppressed discussion.

The salient feature of a right to digital privacy is a safeguard of personal autonomy and dignity. Around the digital world that is, constantly gathering and examining personal data, personal autonomy and dignity can be undermined; the right to digital privacy consequently allows individuals to make purposeful decisions regarding the information they share and with whom they are sharing such information, reducing the potential threats of targeted discrimination or exploitation.

The right to digital privacy is one of the human rights that must be acknowledged. The right is being guarded by current international law and relevant international resolutions and homeland law ought to be taken into consideration. Privacy as a human right is inalienable, non-derogable and indivisible.² It does not lapse or abate because of non-use.¹

¹ Hossam El-Din El-Ahwani, *The Right to Respect for Private Life*, Dar Al-Nahda Al-Arabiya, Cairo, 1978.

² Houry Omar, *Constitutional Law*, Al-Halabi Legal Publications, Lebanon, 2009, pp. 160-161.

The protection of personal information, freedom of expression, autonomy, and dignity of people in the digital era is based on the right to digital privacy as a key human right. It is important to make sure that governments, businesses, and other stakeholders adhere to and honor this right to ensure safe and secure movement on the digital milieu.

Finally, the digital privacy right plays a crucial role in democratic, human, and rule of law in the digital era. Business, governments and civil society are therefore required to continue being committed to upholding this right in order to promote trust and accountability in digital ecosystems.

As a result, the paper will discuss in the first section the role of artificial intelligence on the right to digital privacy, and in the second section, the regulations provided by law in safeguarding the right.

3.1 The Impact of Artificial Intelligence on the Right to Digital Privacy

In modern culture, where the rate of the technological revolution is very high, artificial intelligence (AI) has become one of the most effective tools that can impact the right to the digital privacy on a great scale. With AI technologies (such as machine-learning algorithms and facial-recognition software) having the ability to collect and process large amounts of personal information, it raises serious questions about the process or protection of the rights of people to have their digital privacy. It, therefore, follows that the implications of AI on the right to privacy holistically, and an evaluation of the advantages and disadvantages that it presents in the context of privacy-related rights is justified.

It is difficult to come up with the accurate definition of privacy, but, still, jurisprudence has identified a number of parameters that should be met to consider the concept in question a safeguarded right. The jurisprudential analysis further examines the difference between an objective conception of privacy; it concerns a personal life, and the relative conception, it depends on dynamism of life and hence it differs on individuals, places, and the time.² A right can be understood as a capability of legally granted to an individual within a certain domain, and in which this capability is the

¹ Sabrina Ben Said: Protecting the Right to Privacy in the Age of Technology, PhD Dissertation, Faculty of Law and Political Science, University of Hadj Lakhdar, Batna, 2014/2015, p. 23.

² Husam al-Din al-Ahwani, The Right to Respect for Private Life, Dar al-Nahda al-Arabiya, Cairo, 1978, p. 4.

nature of the right whilst creating a dynamic of relation that empowers the possessor and places a duty on an outsider; the same applies to the right of privacy.¹

One of the benefits of AI that are the most relevant is its ability to enhance the security systems and protect confidential data. The risk of unauthorized access to personal data can be prevented because AI-powered cybersecurity systems are able to monitor and address the possible threats in real-time. This capability will protect the digital privacy of the people by ensuring that their data is not exposed to malicious individuals who could take advantage of the underlying weaknesses within these systems. Furthermore, AI can be used to automate privacy-compliance processes, and this will ensure that organizations comply with the current data-protection laws and regulations.

In its turn, the introduction of AI in data collection and analysis generates substantive issues concerning the loss of digital rights of individuals in the context of their privacy. Artificial intelligence programs periodically spy and trace the online actions of users, thus creating an online footprint that can be exploited in the commercial sector or to ensure surveillance. Such usage may trigger a loss of privacy and control of personal data hence violating the right to privacy of individuals. The use of AI in facial - recognition technologies has also sparked controversy regarding the ethical consequences of mass surveillance and the misuse of biometric data.

Policymakers and agencies should predict the safeguarding of the right to digital privacy of individuals when developing and deploying AI technologies to alleviate such challenges. This will involve bringing in strong data-protection measures, including encryption and anonymization, to keep individual data out of unethical use. Also, transparency and accountability mechanisms are to be established whereby people will be properly notified about the mediums according to which their data are gathered, processed, and used by AI systems.

The influence of AI on the digital privacy right is a multifaceted question that needs careful consideration and active interventions to protect the rights of people. Even though AI has the prospects of facilitating security

¹ Abdul Karim Alwan, *The Mediator in Public International Law*, Book Three: Human Rights, Dar al-Thaqafa for Publishing and Distribution, Amman, First Edition, 2010, p. 110.

and optimizing administrative operations, it also contains some hidden dangers to privacy by collecting and spying on large amounts of data. These issues can be implemented by adopting strict data-protection measures and ethical standards to explore the potentials of AI without sacrificing the digital privacy of people in an ever-growing interconnected global environment.

Ethics acts as the guide to morality in the development of AI and data privacy, guiding the developers on intricate data acquisition and algorithmic decision-making. Without ethical considerations, AI systems are bound to become a force that does not serve but aims to monopolize its users. Based on the principles of transparency up to the principles of fairness, these normative doctrines require AI to be thought and implemented in ways that do not infringe on the digital rights of individuals and that do not precondition the commercialization of personal data.

Data privacy is not just a checklist, but it is an ethical requirement in the age of ubiquitous artificial intelligence. Since AI systems gradually enter the everyday routine, the security of personal information goes beyond the legal compliance to the protection of fundamental rights and the humane treatment of information. Although attempts to protect the privacy of digital data in AI systems have been made, there are latent issues and threats that current systems have yet to tackle, making the use of the AI environment a high-stakes game.

The data security deficiencies of the AI applications are comparable to leaving an unlocked front door to a neighborhood full of cyber-thieves. Between attackers, taking advantage of flawed systems to intrusions that lead to massive consequences the security of personal data in the AI ecosystems is the most important aspect since stealing the data can cause disastrous outcomes.

The use and unwarranted obtaining of personal data without reasonable disclosure is one of the most significant issues in AI-driven digital privacy. Even though AI systems tend to rely on the large volume of data as a prerequisite of effectiveness, this reliance must not override the privacy expectations of individuals. In this regard, organizations and developers should be keen on user-data security and have rightful controls in place to prevent unlawful access or abuse. Without strong security measures, sensitive data can be leaked or modified without any permission.

The ability to have personal privacy in the AI context is essential in maintaining trust and accountability in technology. Since AI is penetrating various fields, such as healthcare, finance, and law enforcement, the trust in protecting personal information is paramount.¹ By adhering to the right to privacy, organizations can exercise ethical stewardship and ensure, by doing this, that the individual retains control over the use of his or her information. Therefore, the protection of digital privacy in the field of AI is not only a legal or moral imperative but a critical step in the creation of a more secure and trustworthy digital world.

Digital privacy, which is a more specific term than privacy, involves the wise management and use of sensitive data, especially the personal information, communication, and records of behaviour created and exchanged in the digital setting. Essentially, the nature of digital privacy is related to the rights and expectations of people to preserve privacy and security of their personal information on the digital platform. Therefore, digital privacy is one of the strongest forms of protection, and it sets the clear lines that may ensure that the users are not affected by the random data breaches and manipulations that could lead to the loss of the human dignity and personal will.

No less significant is the contribution of digital privacy towards the preservation of a strong democratic society. It enables the freedom of thought, expression and instills a pluralistic continuum of ideas and opinions. In the business sphere, carefully designed digital privacy policies increase consumer confidence and corporate goodwill, which is invaluable to long-term growth and business competitiveness in the modern market. The fact that data breaches have been committed is sealed by the presence of strict privacy camouflage; and as the rate of cybercriminal activity is on a rise, the privacy of the individual digital data has an urgent nature, which explains why the privacy protection is an urgent issue.

The use of emerging technologies, especially artificial intelligence (AI), has a significant impact on digital privacy. The data processing and analytical inference capabilities of AI allow the provision of improved services and draw conclusions, but the same abilities could be used to build

¹ Sabrina Ben Said: Protecting the Right to Privacy in the Age of Technology, PhD Thesis, Faculty of Law and Political Science, University of Hadj Lakhdar, Batna, 2014/2015, p. 16.

a profile and make decisions without substantive human control, thus, posing the threat of unreasonable encroachments of privacy of individuals. Therefore, AI is also a promising enforcer and a threat to the privacy on the Internet, which requires the implementation of broad privacy laws.

Another key trend, data analytics, can be used to inform digital privacy policies as it provides an insight into user behavior and provides a possibility to customize services. However, uncontrolled data gathering and analysis may easily be in violation of the personal privacy. Therefore, data mitigation and anonymization mechanisms should be tied to analytics to balance efficiency and privacy issues. Scientific and technical innovations have given people freedom to seek independence, but at the same time have made personal information accessible and prone to unscrupulous use, theft, misuse of identity, and privacy invasion.

People can become accustomed to the changing digital privacy by keeping pace with all changes in the world of technology and the new privacy-related threats that it causes. The epistemic growth of Internet of Things (IoT) devices in everyday life has serious threats; the devices accumulate, process, and transfer large amounts of highly personal data, which, when used, or not secured, creates massive privacy risks. Based on this, critical research on the prerogative of digital privacy in international human rights laws is urgent in the age of AI.

3.2. Legal Protection of the Right to Digital Privacy

In the age of the saturation of technologies, where people are constantly communicated with, the significance of the right to privacy in the digital world has become even greater. The more people share increasingly broad personal data via the Internet, the more concerns arise about the possibility of its misuse. This has made the protection of this right under the law to become the center of concern among governments and organizations across the world. The advancement in technology and the creation of information repositories has created the concept of information privacy.¹

One of the main modes of ensuring the right to digital privacy is legislation. The majority of the national constitutions do not allow unreasonable searches and seizure, even in the digital world. Additional law like the Electronic communications privacy act and the computer fraud

¹ Omar Al-Hamami, Criminal Protection of Electronically Recorded Information: A Comparative Study, Dar Al-Nahda Al-Arabiya, 2010, p. 825.

and abuse act provides supplementary protection to personal data and internet communications hence form the basic structure of privacy protection in the digital era. The domestic legislation is therefore the right circumscription that should be used to protect this right.¹

In addition to the enactment of bills, the protection of digital privacy requires the implementation of these laws. Governmental organizations and law-enforcement agencies must follow some high-security measures when reading online information of individuals, procurement of a court-order before accessing electronic communications become a condition to adhere to the digital privacy rights. Moreover, organizations gathering and retaining personal data should ensure they have strong security that will exclude unauthorized access. Therefore, the privacy shielding by the specialized legislation is necessary and, in its absence, the judicial system is the qualified body.²

IT enterprises should be of critical importance when it comes to the right to digital privacy. Google, Apple, and Facebook corporations have implemented encryption systems and individualized privacy controls to protect the information of its users against bad actors. They also provide consumers with greater control over the gathering, use and sharing of their information, thus creating transparency concerning data gathering. The technology companies therefore help to enforce the rights to digital privacy in the following ways.

The right to privacy is provided under an elaborate legal framework in the international human rights law. Article 12 of the 1948 Universal Declaration of Human Rights states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."³ The right to privacy is inalienably connected to a range of other interrelated human rights that can be compromised in the context of the personal data gathering, interception of the digital communications, and mass

¹ Sameh El-Tohamy, "Legal Protection of Personal Data: A Study in French Law," *Journal of Law, Kuwait*, Volume 35, Issue 3, 2011, p. 381.

² Ahmed Fathi Sorour, *Constitutional Protection of Rights and Freedoms*, Dar Al Shorouk, 2000, p. 15.

³ The Universal Declaration of Human Rights of 1948.

surveillance. These rights include the right to access, receive and publish information; freedom of opinion and expression; freedom of peaceful association and assembly as well as family life.

Article 17 of the International Covenant on Civil and Political Rights of 1966 (ICCPR) codifies the legal protection of the right to privacy. Article 17 declares that: “(1) no one shall be arbitrarily or unlawfully interfered with in his privacy as well as family, home or correspondence, or unlawful attacked in terms of his honour and reputation; (2) every person is under the right to be legally safeguarded against such interference or attacks.”¹

The states are under legal obligation to offer safeguards against and illegal attacks on the privacy of individuals in accordance with paragraph 2 of Article 17. The above requirement is realized by providing strong procedural protection, including institutional structure and necessary distribution of financial resources, and judicial oversight based on international principles of impartiality, independence, and transparency.

Besides, accessibility of litigation or efficient redresses depends on the safeguarding of the right to online privacy. ICCPR, article 2, paragraph 3(b) requires every wronged person to be assured that the rights that he or she asserts to have been violated will be heard by a qualified judicial, or administrative, legislative, or other statutory body, and a recourse to judicial vindication will be established. States should therefore ensure that capable authorities enable people to have access to useful solutions.

On 18 December, 2013, the United Nations General Assembly passed a Resolution 68/167 on right to privacy in the digital age.² This right has later reaffirmed by Resolution 69/166 on 18 December, 2014.³ Moreover, the United Nations High Commissioner of Human Rights issued a resolution named Resolution 68/167 in a report on the same topic, The Right to Privacy in the Digital Age, which was discussed in a seminar on 24 February 2014.⁴

¹ The International Covenant on Civil and Political Rights of 1966.

² UN General Assembly Resolution 68/167 – The right to privacy in the digital age, A/RES/68/167, 18 December 2013.

³ UN General Assembly Resolution 69/166 – The right to privacy in the digital age, A/RES/69/166, 18 December 2014.

⁴ Report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/27/37, 30 June 2014.

International human rights law does not allow the violation of the right of a person to his own privacy unless such violation is authorized by the law, and the law itself has to be in accordance with the resources of the international human rights conventions and treaties. In the international law, states are allowed to spy on electronic communications on the grounds concerning national security, terrorism, intellectual property, and organised crime, thus using them as the grounds in justification of curtailing individual liberty and eroding privacy privileges.¹ However, international law limits such surveillance activity by introducing regulatory limits on them and requiring that programs be restricted, domestically legislated and monitored by international entities.

One of the key catalysts of the development of a legal framework that protects the right to privacy in the age of artificial intelligence is in line with international human rights law regarding privacy and other associated rights. This compels the international and regional human rights organizations, courts, committees and legal academicians to act in their respective jurisdictions and formulate an executive legal system that is favorable to privacy protection.

In 2015, the Human Rights Council created a new privacy mandate in Resolution 28/16.² It selected a Special Rapporteur on the Right to Privacy who would gather credible data provided by governments, non-governmental organizations, and other organizations that have the expertise on privacy situations and problems. Right to privacy allows individuals to and exercise being an incidental right, i.e. right to develop and exercise personality, identity, opinions as well as participate in political, economic and social as well as cultural activities.

To facilitate and protect privacy, the Special Rapporteur is mandated with the role of scrutinizing government policies and laws on interception of digital communications and the aggregation of personal information. His mandate includes detecting and engaging in the occurrence of unjustified privacy-infringing activities. It also involves facilitating states to develop the most appropriate practices to conform international surveillance with

¹ Ghania Ben Krouidem, Digital Rights – Reality and Challenges, Journal of Comparative Legal Studies, University of Hassiba Ben Chlef, Volume 7, Issue 1, 2021, p. 2041.

² United Nations General Assembly, 28/16. The right to privacy in the digital age, A/HRC/RES/28/16, 1 April 2015.

the rule of law. It finally includes illuminating duties of the private sector in regard to the respect of human rights, as well as facilitating in ensuring that national laws and measures are in line with the global duties and obligations to human rights.

Protection of digital privacy rights cannot be done without national and international cooperation in the modern digital age. Governments, institutions, and technology companies can collectively safeguard the privacy of people online by means of legislations and implementing security measures, ensuring responsible data stewardship, and enacting and enforcing the legislation. Due to the growth of technology, there is need to ensure that the efforts to digital privacy keep up with the changes, thus keeping the citizens trustful of the safety of their data over the internet.

4. Conclusion

The active development of artificial intelligence (AI) has made the privacy rights of digital users one of the most important issues. With the proliferation of AI technologies, into the most intimate aspects of society, such as personalized suggestions to autonomous decision-making models, the need to protect the privacy of an individual has become even more urgent. This paper examines the complex interconnection between AI advancement and online privacy by discussing legal regulations, ethical aspects, best practices and future trends that characterize privacy protection in the age of AI.

The paper has affirmed that the right to privacy is a vital concern in the ever-interconnected world that requires a multipronged approach that includes governments, individuals, business, and international cooperation. We can protect and respect the personal data of the people by enacting strong laws on data protection, educating the masses on the fact, and putting in place proper privacy controls and through international collaboration. The right to privacy is not merely a law and ethical obligation but also one of the key human rights that need to be maintained for the future generations.

4.1 Findings

1. International human rights lays the groundwork of encouraging and protecting the right to privacy. It also promotes effective international and domestic control in cases where the domestic law allows the surveillance of the digital communication and gathering of personal information of individuals.

2. International human rights law requires states to adopt domestic laws that internalize efficient procedural protections and control measures whenever such domestic laws authorize the legal surveillance of digital communications and gathering of personal information of individuals so long as such domestic laws are harmonious with the international human rights conventions and treaties.
3. International law ensures that judicial bodies exercises supervision of the safeguarding of the right to privacy in both national, regional, and international levels and provides individuals with the right to litigate and gain fair remedies to defend their right to privacy in digital form.
4. International human rights law provides that states should take coordinated efforts based on international cooperation and involvement of stakeholders including businesses, civil society organizations, and academic bodies, technology, international human rights law experts, and the business community to increase the level of compliance with its provisions as applied to the protection of the right to digital privacy. This is to address the issues of ensuring the protection of the right to digital privacy.
5. States are required to ensure that their national practices, domestic laws and policies are in line with the international human rights law. In case such laws, policies, or practices are deficient, the states are supposed to make effective procedures to examine and ensure that they fully comply with international law.

4.2 Recommendations

1. Governments must pass multilateral legislations on data protection that will provide clear guidelines on how companies and organizations shall collect, store, and use personal information. These laws must include strict punishments against the infringement of privacy of individuals.
2. People should train themselves about the privacy dangers of technology and social media sites, including how their individual data is gathered and disseminated on the web, and the utilization of privacy controls and encryption utilities. Cyber awareness and proactive strategies help people to protect themselves against any threats and violations.
3. The need to protect the right to privacy cannot be done without international cooperation and coordination since data breaches and privacy violations often cross borders. Nations ought to work together to establish common data protection standards and protocols and co-ordinate to fight

cybercrime and privacy breaches. Due to the exchange of information and resources, governments will be in a better position to tackle global privacy issues and punish those who engage in such activities.

4. Best practices must be used to ensure the right to privacy in artificial intelligence (AI) and put ethical concerns at the forefront in the development of AI and the privacy of data. This demands designing strategies of data minimization, anonymization, consent of users and control of data. It also requires the acceptance of the inherent bias of AI algorithms and datasets and the desire to be transparent in both AI systems and data processing. These actions will guarantee that there is responsibility in case of data privacy breach in AI.

References

- Abdul Karim Alwan, The Mediator in Public International Law, Book Three: Human Rights, Dar Al-Thaqafa for Publishing and Distribution, Amman, First Edition, 2010.
- Ahmed Fathi Sorour, Constitutional Protection of Rights and Freedoms, Dar Al-Shorouk, 2000.
- Fawzi Oussedik, The Problem of Information Technology Between the Right to Privacy and the Disclosure of Professional Secrets, Journal of Legal Studies, Al-Basira Center for Educational Research and Consulting, Issue Two, September 2008, Algeria.
- Ghania Ben Krouidem, Digital Rights – Reality and Challenges, Journal of Comparative Legal Studies, University of Hassiba Ben Chlef, Volume 7, Issue 1, 2021.
- Hossam El-Din El-Ahwani, The Right to Respect for Private Life, Dar Al-Nahda Al-Arabiya, Cairo, 1978.
- Houry Omar, Constitutional Law, Al-Halabi Legal Publications, Lebanon, 2009.
- Nahla Al-Momani, Cybercrimes, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2008.
- Omar Al-Hamami, Criminal Protection of Electronically Recorded Information: A Comparative Study, Dar Al-Nahda Al-Arabiya, 2010, p. 825.
- Report of the Office of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, A/HRC/27/37, June 30, 2014.

- Roaa Saad Al-Qarni, Legal Protection of the Right to Information Privacy, Journal of the Faculty of Islamic and Arabic Studies for Girls in Damanhour, Issue 6, Part 1, 2021.
- Sabrina Ben Said: Protecting the Right to the Sanctity of Life Private Law in the Age of Technology, PhD Dissertation, Faculty of Law and Political Science, University of Hadj Lakhdar, Batna, 2014/2015.
- Sameh Al-Tohamy, Legal Protection of Personal Data: A Study in French Law, Journal of Law, Kuwait, Volume 35, Issue 3, 2011.
- The International Covenant on Civil and Political Rights of 1966.
- United Nations General Assembly Resolution 166/69 - The Right to Privacy in the Digital Age, A/RES/69/166, 18 December 2014.
- United Nations General Assembly Resolution 68/167 - The Right to Privacy in the Digital Age, A/RES/68/167, 18 December 2013.
- Universal Declaration of Human Rights of 1948.
- Younis Arab, The Role of Privacy Protection in Promoting Integration into the Digital Society, paper presented at the Arab Information Ethics Club Symposium, 17-18 October 2002, Amman, Jordan.