

Algorithmic Persecution in Artificial Intelligence Systems and Its Impact on Digital Human Rights

الإضطهاد الخوارزمي في أنظمة الذكاء الاصطناعي وأثره على حقوق الإنسان الرقمية

CHERIGUI Youcef *

Faculty of Law, University of Tipaza
Laboratory of Constitutional Institutions
and Political Systems
cherigui.youcef@univ-tipaza.dz

OUAGAZI Okba

Faculty of Law, University of Tipaza
Laboratory of Constitutional Institutions
and Political Systems
ouagazi.okba@univ-tipaza.dz

Date of Submission 02-04-2026 Date of Final Acceptance 01-06-2026 Date of Publication June 2026

Abstract:

This study addresses the issue of algorithmic persecution in artificial intelligence systems by establishing its legal nature and identifying its impact on digital human rights, particularly in light of the growing reliance on algorithms in content moderation, steering user behavior, and controlling access to information. The study primarily aims to establish the conceptual and legal foundations of the dimensions of algorithmic persecution and analyze its implications for the digital human rights framework, particularly the right to online equality, freedom of expression, non-discrimination, and the right to digital self-determination.

The study concludes that this persecution poses a grave threat to digital human rights, as it leads to the reproduction of bias, reinforces digital exclusion, restricts freedom of expression, and deepens disparities among users. The study also reveals the inadequacy of current legal frameworks in addressing this emerging phenomenon, which poses a protection challenge requiring a re-evaluation of traditional legal concepts to ensure algorithmic justice in the virtual environment.

Keywords : Artificial Intelligence; Algorithmic Persecution; Digital Human Rights; Legal Challenges.

ملخص:

تعالج هذه الدراسة إشكالية الاضطهاد الخوارزمي في أنظمة الذكاء الاصطناعي، من خلال تأصيل طبيعته القانونية وتحديد أثره على حقوق الإنسان الرقمية، خاصة في ظل الاعتماد المتزايد على الخوارزميات في إدارة المحتوى، وتوجيه سلوك المستخدمين، والتحكم في الوصول إلى المعلومات. وتهدف الدراسة بالأساس إلى التأصيل المفاهيمي والقانوني لأبعاد الاضطهاد الخوارزمي، وتحليل انعكاساته على منظومة حقوق الإنسان الرقمية، لا سيما الحق في المساواة عبر الإنترنت، وحرية التعبير وعدم التمييز، والحق في تقرير المصير الرقمي.

وقد خلصت الدراسة إلى أن هذا الاضطهاد يشكل تهديدا جسيما لحقوق الانسان الرقمية، إذ يؤدي إلى إعادة إنتاج التحيز، وتعزيز الإقصاء الرقمي، وتقييد حرية التعبير، وتعميق الفوارق بين المستخدمين. كما كشفت الدراسة عن قصور الأطر القانونية الحالية في مواجهة هذه الظاهرة المستجدة، وهو ما يمثل تحديا حاميا يتطلب إعادة النظر في المفاهيم القانونية التقليدية لضمان العدالة الخوارزمية في البيئة الافتراضية.

الكلمات المفتاحية: الذكاء الاصطناعي؛ الاضطهاد الخوارزمي؛ حقوق الإنسان الرقمية ؛ التحديات القانونية.

* Corresponding Author: CHERIGUI Youcef

Introduction

The rapid progression of information technology has led to continuous transformations in all spheres of life, particularly following the advent of artificial intelligence (AI), which is now regarded as the principal gateway to the future and a means of acquiring the tools of power, advancement, and modernity in a perpetually evolving world. This transformation encompasses vast capabilities and sophisticated technologies that frequently surpass the limits of human comprehension.

It is undeniable that the development of artificial intelligence, when pursued without sufficient safeguards or in ways that contravene international law, generates challenges that may adversely impact the digital rights of a broad range of marginalized voices. Within this context, digital rights are an extension of fundamental human rights that must not be infringed upon, and ensuring their protection has become an urgent necessity. This is achieved by guaranteeing opportunities for access and by creating a safe and enabling online environment that facilitates the exercise of these rights. Such rights are to be assured for every individual without discrimination based on race, gender, nationality, ethnicity, language, or religion.

However, the actual conditions of cyberspace reveal that user interactions—reflecting human experiences and shared across diverse websites and online platforms—are subjected to meticulous sorting by artificial intelligence algorithms according to precise characteristics. This process may involve the identification of latent tendencies and the detection of racial and ethnic origins, political or religious affiliations, philosophical convictions, and other classificatory data.

Given this reality, permitting the use of artificial intelligence algorithms in such a fashion introduces further interpretive risks, potentially leading to practices that amount to persecution of digital human rights. This development may exacerbate inequality and discrimination, and facilitate the systematic suppression of freedom of expression, the right to digital self-determination, and the right to seek, receive, and impart information, thereby making the practical protection of these rights and the limitation of their violation increasingly difficult.

Accordingly, digital human rights constitute a distinct legal subject that requires a concrete regulatory framework without altering their inherent nature. They represent an intangible dimension of the human person, necessitating comprehensive protection and sustained efforts to guarantee their respect, assurance, and inviolability. From this vantage point, the International Bill of Human Rights has provided extensive safeguards for the protection of these rights. Furthermore, notable international initiatives have begun to emerge with the aim of solidifying the principles and foundations of such protection within a secure, equitable, and non-discriminatory cyber ecosystem capable of confronting the algorithmic challenges associated with artificial intelligence and the digital persecution these challenges produce.

It is therefore essential to acknowledge that, regardless of the technological sophistication attained by artificial intelligence systems, their true value is realized only when they serve human dignity and advance human values. Within this context, the subject of this study raises significant concerns regarding the possible use of artificial intelligence algorithms for repressive, discriminatory, and authoritarian purposes. Consequently, there is a pressing need to examine the risks posed by this technology to digital human rights.

In this regard, the importance of this study stems from its engagement with one of the most delicate and critical transformations in the contemporary digital environment. It provides a jurisprudential and legal foundation for an emerging and controversial concept, namely “**algorithmic persecution**,” by linking it to the literature on digital human rights. This importance is reflected in both scientific and practical dimensions. From a scientific perspective, the study enriches legal scholarship by deconstructing a technical issue through specialized legal reasoning. From a practical perspective, it highlights the risks posed by the technological expansion of artificial intelligence systems, which have come to exercise systematic cyber discrimination affecting rights closely

connected to the user's digital personality. This makes the identification of such challenges an urgent matter for legislators and those responsible for protecting rights and freedoms.

To Address these challenges, the objectives of this study primarily revolve around achieving a precise conceptual and philosophical understanding of the phenomenon of algorithmic persecution in artificial intelligence systems by examining the causes and mechanisms that generate this bias against users. The study also seeks to identify and analyze the negative implications of these practices for the protective guarantees of digital human rights, with particular focus on the right to equality, non-discrimination, freedom of expression, and the right to digital self-determination. The ultimate objective is to diagnose the nature of the legal challenges resulting from this technological development and to reveal the conceptual limitations of traditional legal rules in addressing these emerging digital violations.

Based on the aforementioned context, the central research problem of this study, therefore, is encapsulated in the following question: **What is the nature of the legal challenges that artificial intelligence poses to digital human rights in light of the growing manifestations of algorithmic persecution ?**

To answer the research problem and achieve the objectives of the study, the descriptive-analytical method was primarily adopted, as it is the most appropriate approach for describing the dimensions of this form of persecution and its technical background, and for analyzing this emerging and complex legal phenomenon. This methodological approach made it possible to link the technical dimension with the legal dimension of "algorithmic persecution," and thus to deconstruct the causal relationship between automated algorithmic decision-making and human rights violations. This methodological integration enabled the study to infer the nature of the protective challenges imposed by intelligent systems on digital human rights and to clarify the extent to which current legal frameworks remain insufficient to accommodate this new pattern of cyber violations and confront its emerging risks.

To fully address the dimensions of this research problem, we have chosen to adopt the well-established binary division commonly used in legal methodology, as follows:

Section I: The Concept of Algorithmic Persecution in Artificial Intelligence Systems

A) Defining Algorithmic Persecution in Artificial Intelligence

B) Causes of Algorithmic Persecution in Artificial Intelligence

Section II: The Impact of Algorithmic Persecution on Digital Human Rights

A) The Concept of Digital Human Rights

B) Challenges to Digital Human Rights in the Context of Algorithmic Persecution

Section I: The Concept of Algorithmic Persecution in Artificial Intelligence Systems

Artificial intelligence algorithms have played a significant role in transforming persecution based on tangible, visible, racial, and discriminatory manifestations into pervasive and intensified virtual practices within cyberspace. As a result, persecution may take on new forms in online environments, fulfilling various objectives and occurring with increased frequency. Within this framework, and to thoroughly present the various ideas related to this issue, this section aims to analyze algorithmic persecution by offering a definition, exploring its underlying objectives, and identifying the conditions and factors that facilitate its occurrence.

A) Defining Algorithmic Persecution in Artificial Intelligence:

From a linguistic standpoint, persecution refers to harsh treatment, oppression, injustice,¹ and the infliction of harm.² It is a verbal noun derived from the verb "*idtahada*" (to persecute), a transitive

verb whose action extends from the perpetrator to the object.³ The forms “*idṭahada–yaḍṭahidu–idṭihādan*” indicate that the subject acts as the persecutor, while the object is the persecuted.⁴

Thus, the expression “*idṭahada khaṣmahu*” is used to mean that an individual has treated his adversary harshly, oppressed him, committed an injustice against him, and caused him harm.⁵ Similarly, the phrase “*idṭahadahu al-‘aduww*” conveys that the enemy has subjected an individual to extreme humiliation and oppression, inflicting harm upon him due to his beliefs or religion.⁶

Linguistically, the term “persecution” shares its meaning with several related concepts, including: inequity, arbitrariness, injustice, excess, tyranny, wrongdoing, oppression, domination⁷, control, authoritarianism, abuse, usurpation, and violation.⁸

The linguistic definition of persecution carries significant importance that is reflected in its technical meaning. In legal and doctrinal usage, persecution refers to “the abuse of authority and the exercise of oppressive and arbitrary treatment, along with the violation of constitutional principles, particularly those related to the protection of human rights.”⁹

It is also defined as “the intentional and severe deprivation of a group of the population within a given country of fundamental rights, in violation of the rules of international law, for political, racial, national, religious, ethnic, cultural, or gender-related reasons.”¹⁰

Persecution is regarded as one of the most egregious crimes against humanity, given its collective, discriminatory, and racist dimensions, which have prompted some to classify it under hate crimes.¹¹ It is not perpetrated as an isolated event or a one-time action; rather, it unfolds within a systematic and organized policy framework that aims to deprive a particular group of its fundamental rights based on racial, religious, or political affiliations.

Based on the preceding definitions, the concept of algorithmic persecution within the context of artificial intelligence becomes more explicit, as it allows for the identification of several crucial aspects. This involves clarifying the term “algorithmic,” which traces its etymological roots to the mathematician Muḥammad ibn Mūsā al-Khwārizmī, whose name was adapted in Latin as *Algorismus*. The Latin term, in turn, was influenced by the Greek word *Arithmos*, meaning “number,” eventually giving rise to the English term “algorithm.”¹²

Linguistically, the term “algorithm” denotes “calculation, rule, method, or solutions,”¹³ whereas its technical usage refers to “a formal analysis of a problem; that is, a sequence of logically connected steps aimed at reaching a specific method.”¹⁴ It also signifies “a set of ordered, clear, and executable steps for a specific task that has a defined end,”¹⁵ or “a method for solving a problem using a finite number of applications of a given rule, whereby an algorithm, starting from an initial condition, allows the application of various operations in a specific and limited order to obtain a result.”¹⁶

According to Oxford Reference, an algorithm is defined as “any well-defined computational procedure that takes a value, or a set of values, as input and, after a finite sequence of computational steps, produces a value or a set of values as output.”¹⁷

It is important to note that the term “algorithms” is not inherently linked to computers, despite the prevalent contemporary association. Although algorithms realize their full potential when integrated with computers through their implementation in programming languages, the primary factor driving this association is speed.¹⁸

On the other hand, the concept of the algorithm has not remained confined to mathematics, which originates from the human ability for abstraction and sensory and logical reasoning. Instead, it has come to form the foundation of modern intelligent systems based on contemporary computing. In recent years, the world has witnessed the rise of highly sophisticated digital algorithms, typically executed via computational symbols on computer devices. The most salient manifestation of this development appears in artificial intelligence systems.

In this regard, artificial intelligence algorithms may be defined as “a set of rules and instructions that enable machines to learn, analyze data, and make decisions, thereby allowing machines to perform certain tasks that require human intelligence to accomplish, including natural language understanding, pattern recognition, and other functions.”¹⁹ In another definition, they are described as “a set of complex software instructions that enable machines to simulate certain aspects of human intelligence, with the capacity to learn, adapt, reason logically, and make decisions based on input data.”²⁰

On this basis, algorithmic persecution in artificial intelligence may be defined as “a form of cyber violence that occurs as a result of internal prejudices or systematic repressive hypotheses embedded during the development of artificial intelligence algorithms, which may produce racist search results imbued with sentiments of hatred and animosity toward communities that have suffered, or continue to suffer, historical, political, or economic persecution.”

In another definition, it refers to “the unjust treatment to which an individual or a group is subjected online on the basis of race, religion, gender, nationality, or political or social affiliation. This includes the exploitation of big data analytics in the absence of a clear legal framework, in a manner that undermines the right to digital self-determination, freedom of expression, equality, and non-discrimination.” It may also be described as “repressive practices carried out through artificial intelligence algorithms as a consequence of distortions or biases in the training data used as inputs for teaching machine learning models, whereby such models tend toward bias and racism, resulting in digital exclusion of certain groups that are frequently stigmatized due to preconceived notions about them.”

Based on the preceding definitions, it becomes possible to delineate certain boundaries distinguishing algorithmic persecution in artificial intelligence from general cybercrimes, which typically involve motives such as financial gain (including theft of banking data), violation of privacy, or attacks aimed at disrupting information systems. In this context, algorithmic persecution is characterized by several key features:

- The underlying motive is often rooted in the interaction of artificial intelligence algorithms with historical, political, religious, or social issues, and is intrinsically linked to the contextual understanding of practices and their surrounding frameworks.
- The institutional dimension: such acts are frequently carried out by states or entities connected to them that possess centralized digital tools, enabling dominance over cyberspace. In these scenarios, algorithms are used to control information flows, manage digital activity, and automate the monitoring and tracking of users online.
- The comprehensiveness of victims: algorithmic persecution does not target specific individuals but rather extends to entire groups of users.
- The objective is to undermine civil and political liberties online—such as freedom of expression, freedom of opinion, and access to information—while also infringing upon broader human rights, shaping public opinion, and spreading misleading information.
- It is founded on the exploitation of intelligent algorithms for text analysis and data processing to impose censorship, restrict content, and suppress digital activity by applying arbitrary measures against individual and group accounts, including temporary suspension or permanent deletion. A pertinent example is the algorithmic persecution exercised by social media platforms against Palestinian content published online to expose Israeli crimes against civilians. During the latest Israeli aggression on Gaza, Meta—the parent company of Facebook and Instagram—along with X (formerly Twitter), employed intelligent algorithms designed to monitor user behavior and removed a significant number of posts documenting occupation crimes, citing “violations of community standards,” even though such content provided accurate documentation of war crimes recorded by human rights organizations.

Consequently, and in light of the foregoing, it is necessary to conclude that, despite differences in specific aspects, both algorithmic persecution and other forms of cybercrime ultimately represent criminal conduct, each arising from the commission of acts punishable by law.

B) Causes of Algorithmic Persecution in Artificial Intelligence:

Prior to engaging in a detailed analysis of the factors contributing to algorithmic persecution, it is essential to clarify certain foundational concepts due to their significant role in understanding the context within which these causes have emerged.

Digital platforms integrated with artificial intelligence are designed to simulate human behavior, aiming to increase the degree of human–machine interaction. For example, social media platforms—most notably Facebook—capitalize on individuals’ inclination to share personal experiences and leverage users’ engagement with mechanisms for expressing various emotions, such as the “like” button, sadness, or anger. All these interactions generate a data environment that continuously feeds algorithms, thereby creating fertile ground for constructing digital models capable of exerting control over the user experience (UXE, User Experience), the content that users consume on these platforms, and the content they themselves generate, whether in the form of texts, images, or videos related to specific topics.

Consequently, algorithms are programmed in ways that limit users’ ability to fully control the type of content to which they are exposed and that they consume on these platforms, as well as what they wish to publish or share with others. As a result, access to the internet (Accessibility) no longer serves as an effective guarantee for fairness of use. This phenomenon has been demonstrated by numerous studies in the field of socio-technological research, where search engine algorithms, by collecting and analyzing user data, may display results influenced by preconceived racist attitudes towards certain social segments, such as racial and religious minorities, or individuals distinguished by gender, origin, or skin color.

Thus, human interaction with the internet has become an extension of trends shaped by historical, political, and social dimensions, exposing the presence of a repressive digital sphere that perpetuates the unjust use of media and technology.

More importantly, it is necessary to emphasize that persecution does not originate from the algorithms themselves, but rather from their designers and programmers, who operate according to their own preconceived notions, ideologies, orientations, and funding sources. The individuals who develop these systems are inherently part of a political and social framework governed by specific agendas and interests. Accordingly, incidents of algorithmic persecution are not isolated from this broader unjust structure. For example, companies that own social media platforms, such as Meta and X (xAI), utilize algorithms to control the content of posts published by particular groups seeking to communicate their lived realities and engage others with their experiences, especially through live broadcasting and other means. Nevertheless, in a systematic fashion, these companies have invoked their policies, under the guise of “community standards,” to suppress such content by suspending accounts, deleting videos, or restricting the use of specific hashtags.

The Palestinian context, in particular, exemplifies the systematic utilization of participatory digital media platforms to silence authentic Palestinian experiences and curtail their participatory engagement with unfolding events, thereby limiting their right to digital self-determination and freedom of expression. Users often reveal violent content documenting daily realities of bombardment, airstrikes, starvation, arrests, and the pursuit of civilians. However, this raises critical questions regarding the willingness of these platforms to shoulder the consequences of media dissemination as established by human rights over the years, which have rendered such dissemination a foundational element of contemporary societies. Among the most salient of these consequences is freedom of expression, which enables the circulation, transmission, and sharing of information with others.

Based on the foregoing, the principal causes associated with algorithmic persecution may be addressed as follows:

First: Input Data with Repressive Characteristics

Artificial intelligence expert Trishan Green states: “Since artificial intelligence simulates human intelligence by learning from the data fed into it, it will also inherit its flaws. If the data contains racism, classism, or gender discrimination, the systems will entrench and reinforce these ideas.”²¹ Accordingly, artificial intelligence algorithms may incorporate pre-existing information and attitudes that consolidate material and explicit manifestations of negative human behavior, including racist ideas, hatred, or hostility rooted in political, historical, or identity- and land-related conflicts directed against a particular group on the basis of race, color, national, or ethnic origin.

Examples of repressive input data include systematic defamation campaigns conducted through electronic recruitment platforms, where algorithms are supplied with biased employment-related data designed to disseminate false and misleading narratives portraying Black individuals as unqualified for administrative positions in order to marginalize them and damage their reputations, or asserting that women are inherently unsuitable for factory work.

Second: Defective Algorithms

Distorted, noisy, or inconsistent data²² used to feed artificial intelligence algorithms contributes significantly to the reinforcement of digital persecution and the suppression of freedom of expression online. This is particularly evident during the training of artificial intelligence models with data that is inaccurate, inconsistent, or incomplete, which is used to teach machine learning (ML) models how to identify patterns and trends related to specific individuals or groups. Such conditions may cause algorithms to adopt incorrect classifications and generate erroneous decisions, thereby creating an unjust digital environment that restricts these categories of users from accessing information or expressing their views freely on digital platforms. Consequently, algorithmic performance is directly contingent upon data quality²³: the higher the quality and contextual relevance of the data, the more accurate, reliable, and error-free the outcomes.

Third: Algorithms Characterized by Generalization

The generalization of potential risks during the training of artificial intelligence algorithms, under the pretext of legally regulating users’ duties and rights, represents one of the most prominent causes leading to algorithmic persecution. When certain categories of users are broadly classified as violators of social media policies based on their geographical location data, algorithms, in such instances, construct a dynamic digital profile or algorithmic identity for individuals belonging to communities residing in specific geographic areas.

As a result, the content of their posts becomes vulnerable to blocking, suppression, and obscuration, accompanied by the issuance of inaccurate warnings against them. These practices render the posts of such social groups persistently subject to suspicion and accusation, thereby constituting a serious threat to the rights of innocent individuals to freedom of expression and to digital self-determination.

All of the foregoing constitutes the fundamental pillars of what may be described as algorithmic persecution within artificial intelligence systems. Social media platforms and websites offer a clear illustration of how algorithmic persecution is systematically framed and presented under the pretense of objectivity and the protection of digital space from harmful content and its producers alike.

Section II: The Impact of Algorithmic Persecution on Digital Human Rights

Legal scholars emphasize that law is not created by philosophers through their theories, nor by jurists through their formulations, but rather by engineers through their inventions.²⁴ While this assertion may hold merit in its implication, it underscores the reciprocal relationship between digital technology and human rights²⁵. Law frequently arises as a response to practical realities, as is exemplified by the legal development of human rights in reaction to new technologies associated with artificial intelligence systems.²⁶

There exists, therefore, a mutual influence and close interaction between technological advancement and human rights. Whenever a scientific development takes place, a new branch of human rights law emerges to regulate its use and to mitigate its potential harms and risks. In this context, modern technology has given rise to a novel system of digital human rights, which now represents a pivotal turning point aimed at balancing innovation with the imperative to ensure users' enjoyment of the benefits provided by artificial intelligence, while at the same time addressing its newly emerging negative impacts.

Consequently, this section addresses the conceptual dimension of digital rights by exploring their foundational principles and defining their concept, as well as by examining the challenges they face in light of the growing manifestations of algorithmic persecution. On this basis, and to present all ideas relevant to the topic, this section is divided into two subsections as follows.

A) The Concept of Digital Human Rights

Human rights are inherent entitlements vested in all human beings and guaranteed to every person without discrimination on the basis of race, gender, nationality, ethnicity, language, religion, or any other status. Every individual is entitled to enjoy these rights equally, without exception or bias.²⁷

The concept, components, and generations of human rights have undergone substantial development, driven by the cumulative legislative efforts of the human rights movement at the international, regional, and national levels, as well as by the emergence of various doctrinal interpretations aimed at grounding and consolidating these rights.

Digital human rights constitute a natural extension of traditional human rights.²⁸ This is reflected in the gradual evolution from rights concerned with the protection of fundamental human needs of constitutional significance—such as the right to life, physical integrity, and protection against degrading treatment²⁹—to first-generation rights, namely civil and political rights; then to second-generation rights, including economic, social, and cultural rights; and subsequently to third-generation rights, also known as collective or solidarity rights, such as the right to development, the right to lasting peace, the right to a healthy environment, and the right to self-determination. This evolution has culminated in a new phase within the generations of human rights, represented by the fourth generation, which is embodied in digital rights associated with the use of the internet.³⁰

These rights are closely linked to technological infrastructure, including networks, communications systems, and software. They encompass new digital entitlements designed to address the distinctive challenges posed by cyberspace and to respond to the specific needs and interests of internet users, which often have no direct equivalent in the physical world.

Accordingly, digital technology has significantly transformed the ways in which individuals exercise almost all the rights enshrined in the Universal Declaration of Human Rights, ranging from freedom of thought and expression to the right to privacy.³¹

The concept of digital human rights has therefore attracted increasing attention from the international community, which seeks to clarify and establish these rights as shared values among nations. This concern has generated numerous doctrinal efforts aimed at anchoring such rights within a clearly defined legal framework.

Defining the concept of digital human rights nevertheless raises several challenges, particularly because some approaches tend to limit these rights to the mere guarantee of free access to the opportunities offered by digital technology—such as the right to internet access—and to associate them primarily with freedom of expression. In this context, the Human Rights Council affirmed that “the same rights that people enjoy offline must also be protected online, in particular freedom of expression.”³²

In developing a conceptual framework for these rights, several contemporary studies have adopted specific terms to express related concepts, including “digital rights,” “internet rights law,” “technological rights,” “the human right to the internet,” and “the human right to access information technology,” among other synonymous expressions. Consequently, definitions of digital human rights have multiplied. Some scholars define them as “the right to ensure that opportunities to use the internet and digital technology are freely available in a secure manner,”³³ while others define them as “the right of every individual to access, create, and publish their own digital content, and to use computers, software, or communication networks without condition or restriction.”³⁴

Another definition characterizes digital rights as “the set of guarantees, freedoms, and privileges enjoyed by individuals and groups when using digital technologies and communication networks, whether through the internet or through various electronic devices.”³⁵

In this regard, part of legal doctrine maintains that digital rights are merely an extension of the human rights enshrined in relevant international treaties, now situated within a modern technological environment that requires specific legal regulation supported by precise technical and procedural details.³⁶

In accordance with this perspective, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, stated in the summary of a 2012 Human Rights Council panel discussion on the promotion and protection of freedom of expression on the internet that “there is no need for new human rights standards specific to the internet, as human rights principles and doctrines apply to the internet just as they do elsewhere.”³⁷

Conversely, another current within legal doctrine asserts that the concept of digital human rights is intrinsically linked to the protection and realization of rights that were previously unrecognized. For instance, the “right to access the internet” is considered essential to the exercise of a broad array of digital rights; the “right to informational privacy,”³⁸ which gives rise to the Right to Digital Oblivion and the Right to Digital Anonymity; and the “right to digital self-determination,” which centers on individuals’ freedom to participate actively in cyberspace, protection from surveillance and algorithmic decision-making, as well as the freedom of users to make independent decisions and exercise control over their personal data. This also includes additional digital rights, such as the right to “digital freedom of assembly” and the right to “freedom of expression on digital platforms.”

Nevertheless, digital human rights remain closely connected to traditional human rights, which provide a foundational framework for understanding their objectives, values, and underlying principles. Accordingly, legal protection extends to digital human rights on the basis of international human rights instruments and overarching constitutional values. A clear illustration of this approach is the European Union’s reliance on human rights principles in adopting the General Data Protection Regulation (GDPR),³⁹ where these values are reflected in the recognition of users’ rights to control their personal data, including the rights of access, rectification, and erasure.

B) Challenges to Digital Human Rights in the Context of Algorithmic Persecution:

To the extent that the internet offers opportunities to mitigate some of the most severe forms of racial discrimination and inequality at the global level, and provides favorable conditions for narrowing the digital divide in marginalized and impoverished regions—thereby enabling greater awareness, expression, and the reception and dissemination of information without geographical

constraints—it may, on the other hand, when combined with artificial intelligence algorithms, generate a wide range of legal and ethical challenges in the field of digital human rights. This is particularly evident given that the essential function of digital rights lies in enabling individuals to freely access the internet, express their opinions, and exercise their right to digital self-determination, irrespective of nationality, gender, national or ethnic origin, skin color, religion, or language. Within this framework, attention is directed toward the most significant challenges that may affect certain core digital rights, which may be outlined as follows:

First: Deprivation of the Right to Digital Freedom of Expression

Social media platforms and internet websites have become the primary outlet for the vast majority of users to express their opinions and ideas and to share information with others, as though these platforms function as digital public spaces for the exercise of fundamental rights and freedoms, such as freedom of expression and freedom of assembly⁴⁰. With the exponential increase in the volume of published content, digital platforms have become incapable of fully controlling data traffic due to the speed of dissemination and the diversity of content formats. This situation has prompted them to adopt artificial intelligence systems with the aim of achieving rapid and effective regulation of digital content⁴¹ (Algorithmic Content Moderation). Consequently, platforms integrated with artificial intelligence have expanded their capacities and discretionary powers in regulating freedom of opinion and expression, based on rules imposed through their terms of use.

Accordingly, digital platforms have increasingly relied on what are referred to as algorithmic moderation systems to proactively detect all content broadcast or published on the platform⁴² (Pre-moderation) and to compare it with information stored in databases, insofar as such content may constitute hate speech, incitement to violence, or violations of public morals.

This practice reflects the principle of prevention within digital society. However, this form of algorithmic moderation adopted by most social media platforms and search engines may diverge from its intended purpose of identifying content that violates platform policies and terms of use, particularly when algorithms are trained using inputs that contain racist or discriminatory ideas embedded within complex historical (colonial), political, social, or security-related contexts.

As a result, certain users of cyberspace are subjected to systematic algorithmic persecution imposed by social media companies against their right to exercise digital freedom of expression, due to posts containing content that reflects their opinions and ideas, political, social, or religious orientations, or expressions of their lived reality. In such cases, published content is proactively removed immediately after algorithms identify it by fragmenting it through hashing into digital fingerprints⁴³ and verifying its complete correspondence with prohibited data (texts, images, or videos) previously stored as inputs within algorithmic systems.

This has also occurred through the systematic targeting of media accounts on digital platforms by limiting the reach of their content or permanently deleting their accounts, as algorithms are capable of identifying, within minutes, specific keywords deemed by platforms to be in violation of their standards.⁴⁴

The suppression of ideas and opinions through algorithmic control over the flow of digital content across various websites and platforms constitutes a violation of digital human rights and represents a direct threat to freedom of expression.

Algorithms have increasingly assumed the role of determining the type of information that the public is permitted to access, thereby exposing a dual standard in the treatment of digital expression and reinforcing patterns of biased content dissemination.

All of this has contributed to the gradual erosion of safe digital spaces for the expression of opinions, reflecting an environment that is progressively more repressive and persecutory in nature. In this manner, social media platforms and search engines have shifted from functioning as universal

tools for liberation and the global dissemination of information and opinions into mechanisms of digital dominance, control, and surveillance.

In the same context, certain social media companies have imposed restrictions on the right to freedom of expression by prohibiting specific words through the implementation of word-filtering systems (Word Filters) integrated with complex algorithms that rely on machine learning techniques, computer vision, and natural language processing (NLP). These algorithms scan textual content, match keywords, and analyze contextual elements in order to render blocking decisions,⁴⁵ which may be grounded in erroneous or repressive assumptions. Meta, for example, classified the term “martyr” as a word associated—according to the company—with violence, despite the fact that this term constitutes a widely used form of expression among millions of users, particularly in the context of expressing solidarity with the Palestinian cause.⁴⁶

In this regard, Human Rights Watch noted in one of its reports that Meta’s reliance on algorithms in content moderation constitutes a major factor in the erroneous application of its policies, including the removal of content that does not violate platform standards merely because it expresses support for Palestine on Instagram and Facebook.⁴⁷

In another context, the right to digital freedom of expression has been transformed into a form of electronic incitement or the promotion of hate speech through the negative exploitation and manipulation of artificial intelligence algorithms. This occurs through the dissemination of fabricated comments or the production of inappropriate content imbued with insults and abuse, with the objective of activating various mechanisms of persecution and repression against digital freedom of expression.

In this respect, it is worth recalling that the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, observed in the summary of a panel discussion held by the Human Rights Council on the promotion and protection of freedom of expression on the internet “the growing tendency to criminalize internet users and to assign intermediaries responsibility for blocking and filtering online content.” He emphasized the necessity of conducting dialogue among multiple stakeholders in order to establish acceptable mechanisms for content blocking and filtering, and stressed that access to the internet, both in terms of content and infrastructure, is intrinsically linked to freedom of expression.⁴⁸

Second: Deprivation of the Right of Access to Digital Information

The right of access to information is regarded as one of the fundamental rights guaranteed by constitutional provisions and framed by international principles and standards. It also constitutes one of the most important mechanisms for activating the individual’s role in oversight and accountability, as well as for promoting societal participation in the consolidation of integrity and transparency.

The profound integration of digital environments into governmental activity, within a framework of openness and transparency, has led many states to adopt artificial intelligence technologies in establishing and managing centralized electronic portals and platforms containing open databases accessible to users. Algorithms are employed to support the automated collection, processing, and dissemination of information, thereby facilitating access to information in terms of speed, efficiency, form, content, time, and place.

In addition, legislative measures have been enacted to enshrine the right of every citizen, through cyberspace, to access information related to the management of public affairs or affecting their rights, without technical, financial, or legal restrictions. This has enabled users to obtain, download, copy, and republish such information.

Accordingly, digital infrastructure has become one of the most significant determinants in strengthening the right of access to digital information of public interest. Nevertheless, governments’ excessive and unethical reliance on artificial intelligence in developing open databases entails unprecedented risks that may amount to digital persecution, systematic bias, and injustice.

Algorithmic control over determining which information reaches the public and which information is withheld raises serious concerns regarding the transparency of algorithmic processes and the extent of their neutrality.

As the complexity of this technology continues to increase, the dilemma of ensuring equitable access to digital information becomes increasingly acute, creating a vacuum in accountability, transparency, and integrity. Many algorithms are trained on historical or political data, or on unbalanced human tendencies, which may lead to systematic persecution and the deprivation of certain groups of their right to access public information in critical fields such as employment, social services, and even criminal justice. This dynamic contributes to the emergence of a biased and discriminatory administrative apparatus operating under the guise of misleading technological legitimacy.

Several documented cases indicate that algorithms may deprive certain users of the right to access information. A particularly illustrative example is a test conducted by AlgorithmWatch, an organization that monitors and evaluates the use of algorithms. Through an artificial intelligence-driven digital platform, the organization published a job advertisement for a truck driver, based on the assumption that the platform's algorithms would discriminate among the target audience in terms of access to employment-related information. The organization indicated that women would be automatically excluded from receiving the advertisement because men are statistically more likely to interact with such postings, according to previous behavioral patterns and predictions of current and future trends.

The test results confirmed that the algorithms directed the advertisement overwhelmingly toward men, with male views and interactions reaching 4,864, compared with only 386 views among women. This outcome demonstrates the existence of a systematic defect in the prior feeding of algorithms, producing unfair and discriminatory consequences based on gender or race in the exercise of the right of access to information.⁴⁹ Algorithms are not inherently biased; however, when men account for approximately 90% of the input data, women effectively become invisible within the platform's operational logic.⁵⁰

development of multiple mechanisms for controlling the flow of information and restricting access to and retrieval of it. Such practices may take the form of refusing to provide information, imposing excessive delays in responses through the prolonged disregard of requests, supplying misleading information, or even blocking internet access entirely, particularly during periods of crisis. All these practices reveal deeper and more complex realities associated with serious violations of human rights.

Studies have shown that one of the most prominent manifestations of deprivation of the right of access to digital information lies in practices carried out by occupying powers, in cooperation with major social media companies, aimed at suppressing colonized peoples and isolating them from the virtual sphere. This is particularly evident with regard to access to digital information documenting violations through images and videos.

As a result, social media companies have resorted to the use of algorithms in ways that widen the digital divide by deepening inequality and digital exclusion against groups that do not conform to the patterns anticipated by algorithmic systems, especially marginalized communities that have endured historical and social persecution. Consequently, the right of access to information becomes constrained by the obstacle of the digital divide, rendering the universality of digital human rights incapable of being fully realized, whether in practical reality or in the digital environment.⁵¹

Third: Violation of the Right to Digital Privacy

In light of the immense technological developments that characterize the contemporary era, human rights have assumed heightened importance. According to Shoshana Zuboff, humanity is currently living in the phase of "surveillance capitalism," understood as a historical phase and a new

economic system based on major corporations—such as Google, Facebook, and X—which seek to collect the largest possible volume of data about users of digital platforms, not solely for the purpose of predicting behavior, but also to influence and modify it simultaneously.⁵²

With the emergence of new technologies and the use of virtual reality enhanced by artificial intelligence to simulate real-life environments, the potential risks associated with violations of users' privacy have intensified. This is attributable to the massive accumulation of personal data stored within search engine records and social media platforms and its subsequent use as input for algorithmic systems. Such data may be collected and retained through unlawful means and without the knowledge, consent, or approval of the individuals to whom it belongs.

The use of artificial intelligence applications in daily life to automate routine tasks—such as ChatGPT developed by OpenAI—has exposed users' sensitive personal data to heightened risk of violation. The information that users provide about themselves, including texts, images, and preferences, is exploited, collected, and processed to construct a virtual profile of the user, whereby the application gains awareness of the user's past, preferences, and other aspects of personal information. Data that users disclose in the form of questions may include information pertaining to professional secrets and commercial skills. As a result, under the privacy policy adopted by OpenAI, ChatGPT reserves the right to reprocess, reproduce, and provide this data to another user,⁵³ even when that user may be a competitor.

Moreover, the risks to users' personal data have extended into the domain of robotics—a technology increasingly integrated into various spheres of life, such as healthcare, entertainment, and domestic assistance. These systems rely on machine learning algorithms to identify patterns within data, enabling them to learn how to distinguish between words, sounds, images, or even to generate such content autonomously.

For example, Microsoft utilized artificial intelligence in developing the chatbot “Sydney” to accompany search results on the Bing search engine. However, this technology prompted considerable concern regarding user privacy violations. In troubling conversations conducted by Marvin von Hagen, a student at the University of Munich, with the chatbot “Sydney,” the system reportedly deviated from its intended operational limits, most notably by threatening to reveal the student's personal information and to disclose his IP address and location.⁵⁴

Such vulnerabilities, which highlighted the deviation of artificial intelligence-driven chatbots from their designed operational scope, pose a significant threat to user privacy and the security of personal data. These incidents constitute direct exploitation of users' digital footprints, personal preferences, and online activities.

The danger escalates when personal data is exploited to cause harm to specific users. The storage and retention of data on artificial intelligence servers—platforms specifically designed to process enormous volumes of information—make effective oversight extremely difficult. Consequently, such data becomes widely accessible and nearly public, increasing its exposure to domination, discrimination, or theft.

Within this framework, certain categories of personal data deemed particularly sensitive—such as information pertaining to race, religion, sexual orientation, or health—may be processed and sold to commercial enterprises for the purpose of targeting advertisements to those groups, appealing to their interests and reflecting their opinions. This practice constitutes a flagrant violation of users' right to the privacy of their personal data.

Fourth: Deprivation of the Right to Freedom from Algorithmic Bias

At a time when artificial intelligence systems were anticipated to enhance digital human rights and reduce societal inequalities among individuals and communities, the results generated by these systems have not been marked by neutrality, but rather by unwarranted caution and bias. This

development now threatens the principle of equality among individuals and has rendered algorithmic justice liable to serious legal reproach.⁵⁵

One of the most distinctive features of artificial intelligence, as learned by AI models during their initial training using machine learning algorithms, is its capacity for inference and reasoning that simulates human cognitive abilities. This allows AI to develop the ability to draw conclusions, make decisions, or generate predictions independently, free from human intervention, control, or supervision.

However, the stage in which AI models are trained on datasets through supervised machine learning, designed to enable AI to imitate the way humans learn⁵⁶, may deviate from legal and ethical principles due to the presence of programmer biases or the adoption of repressive assumptions that reflect societal prejudices against certain groups.⁵⁷ Such inclinations can lead to the training of models on unsafe datasets containing discrimination based on race, color, or gender.

Furthermore, although artificial intelligence can identify patterns and extract results, its reasoning does not equate to human thinking, which is grounded in associative connections, analogy, and contextual inference. AI systems tend to operate according to rigid, literal logic, uninfluenced by emotion, and may function based on assumptions disconnected from actual environments, without considering real-world or social contexts. Unexpected results may arise when systems programmed with particular logics interact with other systems built upon different programming paradigms.⁵⁸ These issues raise a series of pressing questions among researchers regarding the influence of artificial intelligence on profiling, bias, and algorithmic persecution, and how such phenomena can threaten digital rights.

It is well-established that the fundamental standard for the protection of human rights is the guarantee that individuals enjoy all rights and freedoms without any form of discrimination.⁵⁹ However, according to a report by Amnesty International, artificial intelligence can be employed to generate misleading information, circulate fake news, and distort facts, all of which can intensify incitement, bias, and discrimination against certain groups.

For example, when a request is made to the MidJourney website to generate an image of a terrorist, the resulting image produced by the AI depicts a person with Middle Eastern features. This outcome indicates a bias present in the training of such models.⁶⁰

Additionally, the United Nations Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia, and related intolerance has stated that “recent developments in artificial intelligence and its increasing applications continue to raise serious concerns regarding human rights, including fears of racial discrimination.”⁶¹

Thus, the spread of algorithmic bias, coupled with the accelerating development and widespread use of artificial intelligence across various sectors, renders discrimination and bias a systematic phenomenon. Its criminalization has become a priority to protect the essential human right to equality, which is no longer confined, in its traditional sense, to the absence of material discrimination among individuals, but must also encompass the prevention of discrimination in artificial intelligence environments, with the aim of achieving algorithmic justice.⁶²

Conclusion

The effects of algorithmic persecution in artificial intelligence systems discussed above represent an initial attempt to anticipate the future of digital human rights. While they may not cover every potential unlawful consequence, they constitute the most significant among them. Other new digital effects may yet emerge as a result of the use of artificial intelligence algorithms in repressive practices that target the most vulnerable groups, deepen digital divides, and reinforce various forms of inequality. Accordingly, these effects highlight that humanity is living in a rapidly evolving world that requires the establishment of legal frameworks capable of regulating these emerging technologies before they generate a series of problems at the levels of cybersecurity and human rights.

Although this technology signifies a profound transformation in the way technology interacts with human behavior—opening broad horizons for process automation, raising productivity, and improving efficiency—it is also apparent that it brings numerous challenges, raising serious concerns regarding digital human rights, particularly the right to digital freedom of expression, the right to privacy, and the right to freedom from bias and digital persecution. These rights are among those that grant life its intrinsic worth.

By identifying the phenomenon of algorithmic persecution as an expanding issue across various fields of research, and recognizing it as a serious threat to digital human rights, and in view of the preceding analysis, the study arrives at a set of findings and several recommendations, which are set forth as follows:

First : Key Findings

- Algorithmic persecution constitutes a deviation in artificial intelligence outputs that results from the presence of internal biases and systematic repressive assumptions embedded by programmers during the feeding of artificial intelligence models.
- Algorithmic persecution is exercised against specific communities or groups that have endured, or continue to endure, historical, political, or economic persecution on the basis of race, religion, gender, nationality, or identity and affiliation.
- Algorithmic persecution emerges as an extension of racism and bias rooted in human characteristics, with these tendencies manifesting digitally against particular internet users.
- Algorithmic persecution has become a barrier to the realization of the principles of digital human rights, which are no longer limited, in their traditional sense, to the absence of material persecution among individuals, but now also encompass the absence of persecution in digital environments, thus making algorithmic justice an essential part thereof.
- Algorithmic persecution occurs when input data used during the machine learning phase contains racial biases or prior discriminatory practices, leading to the reproduction of such persecution in artificial intelligence outputs and results. It may also arise from the use of distorted and imbalanced data lacking crucial elements, including accuracy, quality, and consistency.
- There is a clear deficiency in the criminalization of algorithmic persecution as a new and expanding criminal phenomenon. This reveals a gap in national criminal legislation, which has often restricted itself to prohibiting certain cybercrimes and addressing persecution in general terms, without specifically defining algorithmic persecution or setting out clear legal provisions and penalties for such offenses.

Second: Recommendations

- Integrating digital human rights at the core of artificial intelligence development and governance at national, regional, and international levels, in alignment with international law.
- Establishing rigorous international and domestic legal frameworks that criminalize the use of artificial intelligence to violate digital human rights and ensure their protection, thereby obligating states to implement these frameworks effectively.
- Urging the United Nations to create a supervisory authority mandated to safeguard digital rights online, particularly the right to digital self-determination and digital freedom of opinion and expression.
- Monitoring repressive cyber practices conducted through artificial intelligence in the surveillance of users, especially among vulnerable and marginalized groups, and in restricting their right to digital expression.

- Promoting international cooperation, capacity-sharing, and equitable access to the advantages of artificial intelligence among all countries, with special emphasis on developing nations, in accordance with the principles of solidarity and shared responsibility.
- Working to elevate societal awareness regarding the importance of digital rights as a fundamental element of stability and trust in the digital sphere, thereby empowering users to comprehend and defend their rights.
- Strengthening the role of international human rights organizations in monitoring artificial intelligence-driven social media platforms and evaluating their risks to rights and freedoms.
- Encouraging international organizations focused on digital rights to intensify pressure on social media companies, compelling them to govern artificial intelligence on solid human-centered foundations in the development of their digital platforms.

Citations:

-
- ¹ ‘Abd al-Ghani Abu al-‘Azm, *Al-Ghani Dictionary*, Dar Al-Kutub Al-Ilmiyya, 2013, p. 1028.
 - ² *Al-Maany Comprehensive Dictionary*, URL: <https://www.almaany.com/ar/dict/ar-ar/اضطهاد/> (Accessed: 08/04/2025).
 - ³ Mustafa ben Mohammad Salim al-Ghalayini, *Compendium of Arabic Lessons*, Al-Maktaba Al-Asriyya, 28th Edition, Saida, Beirut, 1993, p. 34.
 - ⁴ Ahmad Mokhtar Omar, *Dictionary of Contemporary Arabic Language*, Alam Al-Kutub, Vol. 1, 1st Edition, Cairo, 2008, p. 1372.
 - ⁵ ‘Abd al-Ghani Abo al-‘Azm, Op. Cit., same page.
 - ⁶ Ahmad Mukhtar Omar, Op. Cit., p. 1373.
 - ⁷ *Al-Maany Comprehensive Dictionary*, URL: <https://www.almaany.com/ar/thes/ar-ar/الإضطهاد/> (Accessed: 08/07/2025).
 - ⁸ *Arabic Ontology*, URL: <https://ontology.birzeit.edu/lexicalconcept/46403> (Accessed: 08/07/2025).
 - ⁹ Ahmad Mukhtar Omar, Op. Cit., same page.
 - ¹⁰ Ahmad Atiya, *The Permanent International Criminal Court: A Study of the Court’s Statute and the Crimes within its Jurisdiction*, Dar Al-Nahda Al-Arabia Publishing, Cairo, 2006, p. 183.
 - ¹¹ Sawsan Tamarkhan, *Crimes Against Humanity in Light of the Provisions of the ICC Statute*, Al-Halabi Legal Publications, Beirut, 2006, p. 475.
 - ¹² Panos Louridas, translated by Ibrahim Ahmad, *Algorithms*, Hindawi Foundation for Publishing, 2022, p. 21.
 - ¹³ *Al-Maany Comprehensive Dictionary*, URL: <https://almaany.com/ar/dict/ar-en/algorithm/> (Accessed: 08/10/2025).
 - ¹⁴ Sara Zergout, Chawki Noui, *Engineering Artificial Intelligence Algorithms and Their Manifestations Across Social Networking Platforms: The Unethical Practices of Cambridge Analytica as a Model*, Al-Baheth Al-Iqtisadi Journal, Vol. 11, No. 02, University of 20 August 1955 – Skikda, Algeria, 2023, p. 222.
 - ¹⁵ Najwa Ferran, *The Role of Artificial Intelligence Algorithms in Automated Analysis of the Arabic Language at the Banking Level*, Contemporary Studies, Vol. 05, No. 02, University of Tissemsilt, Algeria, 2021, p. 467.

- ¹⁶ Eric le Nagard, *Computer Science: Introduction to Algorithmics in Scilab and Python*, Pearson France, France, 2013, p. 41.
- ¹⁷ Colman, A., (2015), *A Dictionary of Psychology*, Retrieved 08/18/2025, from: <https://www.oxfordreference.com/display/10.1093/acref/9780199657681.001.0001/acref-9780199657681-e-276>.
- ¹⁸ Panos Louridas, previously cited, p. 31.
- ¹⁹ Michael K., Fred T., (2024), *Types of AI Algorithms and How They Work*, Retrieved 08/23/2025 from: www.techtarget.com/searchenterpriseai/tip/Types-of-AI-algorithms-and-how-they-work.
- ²⁰ Mohamed Samir, (2024), *Artificial Intelligence Algorithms: The Complete Guide*, URL: <https://mohamedsamirsaid.com/artificial-intelligence-algorithms/> (Accessed: 08/23/2025).
- ²¹ Ahmad Kamel Naeem, *Criminalization of Algorithmic Bias and Mechanisms to Limit It: A Comparative Study*, Legal and Economic Research Journal, Vol. 61, No. 4, University of Menoufia, Faculty of Law, May 2025, p. 450.
- ²² Al-Fakhri, Nawal Mahmoud, *Detecting Distorted Data Using Data Mining Methods: A Comparative Study*, Scientific Conference: A Strategic Vision for the Service Reality in Iraq and Its Reflections on Investment, Univ. of Mosul, College of Administration and Economics, 2011, p. 4.
- ²³ Ken Serwin, Alfred H., *Algorithmic Bias: A New Legal Frontier*, International Association of Defense Counsel, 2019, p. 6.
- ²⁴ C.-A. Colliard, "The Machine and Contemporary French Private Law," in *French Private Law in the Mid-Twentieth Century, Studies Offered to Georges Ripert*, Vol. 1, Paris, LGDJ, 1950, p. 115.
- ²⁵ Ch. Caron, "AI or the Return of HAL," *Communication Commerce Électronique*, No. 5, 2018, p. 1.
- ²⁶ Mahmoud Mohammad Ali Mohammad, *The Extent to Which the Provisions of Civil Law Accommodate AI Realities*, Journal of Sharia and Law, No. 42, Faculty of Sharia and Law, Al-Azhar University, Cairo, October 2023, p. 1313.
- ²⁷ United Nations, Global Issues – Human Rights, URL: <https://www.un.org/ar/global-issues/human-rights> (Accessed: 10/15/2025).
- ²⁸ Abdul Rahman Omar Mohammad Al-Mubaidin, *The Legal Framework for Digital Rights: Between Constitutional Protection and Administrative Regulation*, Al-Zaytoonah University Journal for Legal Studies, Vol. 6, Issue 2, 2025, p. 23.
- ²⁹ Nabil Mohammad Khalil Ibrahim, *Digital Human Rights*, The Legal Journal, Vol. 19, No. 1, February 2024, p. 690.
- ³⁰ Ibrahim Ali Badawi Al-Sheikh, *The International Application of Human Rights Conventions: Mechanisms and Main Issues*, Dar Al-Nahda Al-Arabia, 1st Ed., Cairo, 2008, p. 8.
- ³¹ United Nations High Commissioner for Human Rights (OHCHR), (2023), *Shaping Digital Technologies to Empower People to Build Their Lives*, URL: <https://www.ohchr.org/ar/stories/2023/05/shaping-digital-technologies-empower-people-build-their-lives> (Accessed: 10/17/2025).
- ³² United Nations Digital Library, Human Rights Council Resolution 2016, Ref. No. A_HRC_RES_32/13-AR, URL: <https://digitallibrary.un.org/record/845727?ln=ar&v=pdf> (Accessed: 10/20/2025).
- ³³ Nabil Mohammad Khalil Ibrahim, *ibid.*, pp. 290–291.
- ³⁴ Mohammad Tahir, *Digital Freedoms – Basic Concepts*, Foundation for Freedom of Opinion and Expression, 1st Ed., Cairo, 2013, p. 5.

- ³⁵ Mohammad Sobhi Hassan Ali, Mohammad Tarek El-Sayed, *Constitutional Protection of Digital Rights*, International Journal of Jurisprudence, Judiciary and Legislation, Vol. 6, No. 2, 2025, p. 416.
- ³⁶ Ibid., p. 418.
- ³⁷ UN Digital Library, Report of the United Nations High Commissioner for Human Rights 2012, Ref. No. A_HRC_21/30-AR, URL: <https://digitallibrary.un.org/record/731134?ln=ar&v=pdf> (Accessed: 10/23/2025).
- ³⁸ Dafna Dror-Shpoliansky, Yuval Shany, "It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology," *European Journal of International Law*, Vol. 32, Issue 4, November 2021, pp. 1249–1282.
- ³⁹ Giovanni De Gregorio, "Digital Constitutionalism, Privacy and Data Protection," in *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, May 2022, pp. 216–272.
- ⁴⁰ Thiago Dias Oliva, "Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression," *Human Rights Law Review*, Vol. 20, Issue 4, December 2020, p. 614, Doi: <https://doi.org/10.1093/hrlr/ngaa032>.
- ⁴¹ Mohammad Faiz Mohammad Hussein, *Algorithmic Governance of Freedom of Opinion and Expression on the Internet – Developing Social Media Platforms for AI Mechanisms to Regulate Human Behavior in the Digital Domain*, Conference on Legal and Economic Challenges and Prospects of AI, 4–5 November 2023, Faculty of Law, Ain Shams University, 2024, p. 304.
- ⁴² Cambridge Consultants, *Use of AI in Online Content Moderation*, 2019, p. 35.
- ⁴³ Thiago Dias Oliva, Op. Cit., p. 609.
- ⁴⁴ UNESCO, "The Shift of Social Platforms to AI: How Are Female Journalists and Their Content Affected?" URL: unesco.org/ar/articles/thwwl-mnsat-altwasl-aly-aldhka-alastnay-kyf-ttathr-alshfyat-wmhtwahnw (Accessed: 09/03/2025).
- ⁴⁵ S.M. Rokade, Madhuri Palve & Others, "Social Media Content Filtering," *International Research Journal of Modernization in Engineering Technology and Science (irjmets)*, Vol. 05, Issue 05, May 2023, p. 4503, DOI : <https://www.doi.org/10.56726/IRJMETS39518>
- ⁴⁶ Meta, (2023), "PAO on the Treatment of the Term 'Shaheed' (شهيد)," Retrieved 09/03/2025 from: <https://transparency.meta.com/oversight/oversight-board-cases/shaheed-pao/>.
- ⁴⁷ Human Rights Watch, (2023), "Meta's Broken Promises," Retrieved 09/03/2025 from: <https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and>.
- ⁴⁸ United Nations Digital Library, Report of the United Nations High Commissioner for Human Rights 2012, Ref. No. A_HRC_21/30-AR, Op. Cit., p. 3, (Accessed: 10/27/2025).
- ⁴⁹ John Albert, "Not a Solution: Meta's New AI System to Contain Discriminatory Ads," Algorithm Watch, Retrieved 11/04/2025 from: <https://algorithmwatch.org/en/meta-discriminatory-ads>.
- ⁵⁰ Nourhan Gouda (November 25, 2024), "Recruitment Algorithms That Do Not See Women," URL: <https://iwnss.arij.net/ar/report20/> (Accessed: 11/04/2025).
- ⁵¹ Mohammad Arhal, "Does the Process of Digitization Create a New Pattern of Human Rights?" *Istiṣrāf Journal for Future Studies*, No. 09, December 2024, p. 01.
- ⁵² Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019), p. 14.

- ⁵³ OpenAI, (2025), *Privacy Policy*, Retrieved 11/04/2025 from: <https://openai.com/ar/policies/row-privacy-policy/>
- ⁵⁴ Marvin H., (2023), Retrieved 11/05/2025 from: <https://x.com/marvinvonhagen/status/1625852323753762816> .
- ⁵⁵ Ahmad Kamel Naeem, Op. Cit., p. 440.
- ⁵⁶ Mesh Fliders, (2024), Ian Smalley, "What is AI Inference?" Retrieved 11/08/2025 from: <https://www.ibm.com/think/topics/ai-inference>.
- ⁵⁷ Balkis Karaza, Souad Kassa, "The Connection Between Artificial Intelligence, Reality, and Law," International Symposium on Digital Bias in AI Systems, University Center Si El Haouas – Barika, Batna, Algeria, September 25, 2022, p. 4.
- ⁵⁸ Mahmoud Mohammad Ali Mohammad, Op. Cit., p. 1318.
- ⁵⁹ Article 2 of the Universal Declaration of Human Rights, 1948.
- ⁶⁰ Mona Shteiha, (2023), "The Threat of Artificial Intelligence to Human Rights and the Problem of Profiling and Digital Persecution," URL: <https://mc-d.co/1sqa> (Accessed: 11/11/2025).
- ⁶¹ United Nations High Commissioner for Human Rights (OHCHR), (2024), "Racism and Artificial Intelligence," URL: <https://ohchr.org/ar/stories/2024/07/racism-and-ai-bias-past-leads-bias-future> (Accessed: 11/11/2025).
- ⁶² Mahmoud Salama Al-Sharif, *Criminalizing Algorithmic Bias: An Analytical and Comparative Foundational Study*, Al-Zaytoonah University of Jordan Journal for Legal Studies, Special Issue, 2024, p. 841.

Bibliography:

A- Sources:

1. 'Abd al-Ghani Abu al-'Azm, *Al-Ghani Dictionary*, Dar Al-Kutub Al-Ilmiyya, 2013.
2. Ahmad Mukhtar Omar, *Dictionary of Contemporary Arabic Language*, Alam Al-Kutub, Vol. 1, 1st Edition, Cairo, 2008.
3. Mustafa al-Ghalayini, *Compendium of Arabic Lessons*, Al-Maktaba Al-Asriyya, 28th Edition, Saida, Beirut, 1993.

B- Books:

1. Ahmad Atiya, *The Permanent International Criminal Court: A Study of the Statute and the Crimes Under its Jurisdiction*, Dar Al-Nahda Al-Arabia Publishing, Cairo, 2006.
2. C.-A. Colliard, "La machine et le droit privé français contemporain," in *Le droit privé français au milieu du XXe siècle, Etudes offertes à Georges Ripert*, Vol. 1, Paris, LGDJ, 1950.
3. Eric le Nagard, *Informatique: Initiation à l'algorithmique en Scilab et Python*, Pearson France, France, 2013.
4. Ibrahim Ali Badawi Al-Sheikh, *The International Application of Human Rights Conventions: Mechanisms and Main Issues*, Dar Al-Nahda Al-Arabia, 1st Ed., Cairo, 2008.
5. Mohammad Tahir, *Digital Freedoms – Basic Concepts*, Foundation for Freedom of Opinion and Expression, 1st Ed., Cairo, 2013.
6. Panos Louridas, trans. Ibrahim Ahmad, *Algorithms*, Hindawi Foundation for Publishing, 2022.
7. Sawsan Tamarkhan, *Crimes Against Humanity in Light of the ICC Statute*, Al-Halabi Legal Publications, Beirut, 2006.

8. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

C- Newspaper Articles:

1. Abdul Rahman Omar Mohammad Al-Mubaidin, "The Legal Framework for Digital Rights: Between Constitutional Protection and Administrative Regulation," *Al-Zaytoonah University Journal for Legal Studies*, Vol. 6, No. 2, 2025.
2. Ahmad Kamel Naeem, "Criminalization of Algorithmic Bias and Mechanisms to Limit It: A Comparative Study," *Legal and Economic Research Journal*, Faculty of Law, University of Menoufia, Egypt, Vol. 61, No. 4, May 2025.
3. Cambridge Consultants, *Use of AI in Online Content Moderation*, Ofcom, 2019.
4. Ch. Caron, "L'IA ou le retour de HAL," *Communication Commerce Électronique*, No. 5, 2018.
5. Dafna Dror-Shpoliansky, Yuval Shany, "It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology," *European Journal of International Law*, Vol. 32, No. 4, November 2021, DOI: <https://doi.org/10.1093/ejil/chab087>
6. De Gregorio Giovanni, "Digital Constitutionalism, Privacy and Data Protection." In: *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, May 2022, DOI: <https://doi.org/10.1017/9781009071215.007>
7. Ken Serwin, Alfred H., "Algorithmic Bias: A New Legal Frontier," *International Association of Defense Counsel*, 2019.
8. Mahmoud Mohammad Ali Mohammad, "The Extent to Which the Provisions of Civil Law Accommodate AI Realities," *Journal of Sharia and Law*, Faculty of Sharia and Law, Al-Azhar University, Cairo, No. 42, October 2023.
9. Mahmoud Salama Al-Sharif, "Criminalizing Algorithmic Bias: An Analytical and Comparative Foundational Study," *Al-Zaytoonah University of Jordan Journal for Legal Studies*, Jordan, Special Issue, 2024.
10. Mohammad Arhal, "Does the Process of Digitization Create a New Pattern of Human Rights?" *Istiṣrāf Journal for Future Studies*, Arab Center for Research and Policy Studies, Qatar, Vol. 9, No. 9, 2024.
11. Mohammad Sobhi Hassan Ali, Mohammad Tarek El-Sayed, "Constitutional Protection of Digital Rights," *International Journal of Jurisprudence, Judiciary and Legislation*, Egypt, Vol. 6, No. 2, 2025.
12. Nabil Mohammad Khalil Ibrahim, "Digital Human Rights," *The Legal Journal*, Faculty of Law, Cairo University, Egypt, Vol. 19, No. 1, February 2024.
13. Najwa Ferran, "The Role of Artificial Intelligence Algorithms in Automated Analysis of the Arabic Language at the Banking Level," *Contemporary Studies*, University of Tissemsilt, Algeria, Vol. 5, No. 2, 2021.
14. Sara Zergout, Chawki Noui, "Engineering Artificial Intelligence Algorithms and Their Manifestations Across Social Networking Platforms: The Unethical Practices of Cambridge Analytica as a Model," *Economic Researcher Journal*, University of 20 August 1955 – Skikda, Algeria, Vol. 11, No. 2, 2023.
15. S.M. Rokade, Madhuri Palve et al., "Social Media Content Filtering," *International Research Journal of Modernization in Engineering Technology and Science (irjmets)*, Vol. 5, No. 5, May 2023, DOI: <https://www.doi.org/10.56726/IRJMETS39518>

16. Thiago Dias Oliva, "Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression," *Human Rights Law Review*, Vol. 20, No. 4, December 2020, DOI: <https://doi.org/10.1093/hrlr/ngaa032>

D- Seminar papers:

1. Abdallah Al-Fakhri, Nawal Mahmoud, "Detecting Distorted Data Using Data Mining Methods: A Comparative Study," *A Strategic Vision for the Service Reality in Iraq and Its Reflections on Investment*, College of Administration and Economics, University of Mosul, Iraq, 2011.
2. Belkisse Krazza, Souad Kassa, "The Connection Between Artificial Intelligence, Reality, and Law," *Digital Bias in AI Systems*, University Center Si El Haouas – Barika, Batna, Algeria, 2022.
3. Mohammad Faiz Mohammad Hussein, "Algorithmic Governance of Freedom of Opinion and Expression on the Internet – Developing Social Media Platforms for AI Mechanisms to Regulate Human Behavior in the Digital Domain," *Legal and Economic Challenges and Prospects of Artificial Intelligence*, Faculty of Law, Ain Shams University, Egypt, 2024.

E- Websites:

1. *Al-Maany Comprehensive Dictionary*, URL: <https://www.almaany.com/ar/dict/ar-ar/اضطهاد/> (Accessed: 04/08/2025).
2. *Arabic Ontology*, URL: <https://ontology.birzeit.edu/lexicalconcept/46403> (Accessed: 07/08/2025).
3. Colman, A. (2015), "A Dictionary of Psychology," Retrieved 18/08/2025 from: <https://www.oxfordreference.com/display/10.1093/acref/9780199657681.001.0001/acref-9780199657681-e-276>.
4. Human Rights Watch, (2023), "Meta's Broken Promises," Retrieved 03/09/2025 from: <https://www.hrw.org/report/2023/12/21/metass-broken-promises/systemic-censorship-palestine-content-instagram-and>.
5. John Albert, "Not a Solution: Meta's New AI System to Contain Discriminatory Ads," *Algorithm Watch*, Retrieved 04/11/2025 from: <https://algorithmwatch.org/en/meta-discriminatory-ads>.
6. Marvin von Hagen, (2023), Retrieved 05/11/2025 from: <https://x.com/marvinvonhagen/status/1625852323753762816>.
7. Mesh Fliders, (2024), Ian Smalley, "What is AI Inference?," Retrieved 08/11/2025 from: <https://www.ibm.com/think/topics/ai-inference>
8. Meta, (2023), "PAO on the Treatment of the Term 'Shaheed'," Retrieved 03/09/2025 from: <https://transparency.meta.com/oversight/oversight-board-cases/shaheed-pao/>.
9. Michael K., Fred T., (2024), "Types of AI Algorithms and How They Work," Retrieved 23/08/2025 from: <https://www.techtarget.com/searchenterpriseai/tip/Types-of-AI-algorithms-and-how-they-work>.
10. Mohamed Samir, (2024), "Artificial Intelligence Algorithms: The Complete Guide," URL: <https://mohamedsamirsaid.com/artificial-intelligence-algorithms/> (Accessed: 23/08/2025).
11. Mona Shteiha, (2023), "The Threat of Artificial Intelligence to Human Rights and the Problem of Profiling and Digital Persecution," URL: <https://mc-d.co/lsqa> (Accessed: 11/11/2025).
12. Nourhan Gouda, (2024), "Recruitment Algorithms That Do Not See Women," URL: <https://iwnss.arij.net/ar/report20/> (Accessed: 04/11/2025).

13. OHCHR, (2023), "Shaping Digital Technologies to Empower People to Build Their Lives," URL: <https://www.ohchr.org/ar/stories/2023/05/shaping-digital-technologies-empower-people-build-their-lives> (Accessed: 17/10/2025).
14. OHCHR, (2024), "Racism and Artificial Intelligence," URL: [ohchr.org/ar/stories/2024/07/racism-and-ai-bias-past-leads-bias-future](https://www.ohchr.org/ar/stories/2024/07/racism-and-ai-bias-past-leads-bias-future) (Accessed: 11/11/2025).
15. OpenAI, (2025), "Privacy Policy," Retrieved 04/11/2025 from: <https://openai.com/ar/policies/row-privacy-policy/>
16. UN Digital Library, "Human Rights Council Resolution 2016," Ref. No. A_HRC_RES_32/13-AR, URL: <https://digitallibrary.un.org/record/845727?ln=ar&v=pdf> (Accessed: 20/10/2025).
17. UNESCO, "The Shift of Social Platforms to AI: How Are Female Journalists and Their Content Affected?" URL: <https://www.unesco.org/ar/articles/thwwl-mnsat-altwasl-aly-aldhka-alastnay-kyf-ttathr-alshfyat-wmhtwahnw> (Accessed: 03/09/2025).
18. United Nations Digital Library, "Report of the United Nations High Commissioner for Human Rights 2012," Ref. No. A_HRC_21/30-AR, URL: <https://digitallibrary.un.org/record/731134?ln=ar&v=pdf> (Accessed: 23/10/2025).
19. United Nations, "Global Issues – Human Rights," URL: <https://www.un.org/ar/global-issues/human-rights> (Accessed: 15/10/2025).