

AI and Human Rights: Challenges for the European Convention on Human Rights

Author: Bernaziuk Inna

Affiliation: PHEI "European University"

Publication: Конституціоналіст · 2025

Publication date: 2025-07-09

Permanent URL:

<https://constitutionalist.com.ua/ai-and-human-rights-challenges-for-the-european-convention-on-human-rights/>

Author information

Inna Benaziuk

Abstract

Abstract: This article highlights some issues of the growing impact of artificial intelligence technologies on human rights and identifies possible directions for improving the provisions of the European Convention on Human Rights (ECHR) in order to enhance the effectiveness of human rights protection mechanisms in new socio-legal conditions. The author examines the challenges arising from the use of artificial intelligence technologies in the context of observing and protecting human rights guaranteed by the ECHR. The article analyzes key aspects of the interaction of artificial intelligence technologies with the rights to privacy, non-discrimination, the right to a fair trial, and freedom of expression. Special attention is paid to technologies such as facial recognition, predictive policing, algorithmic content moderation, and automated decision-making. Based on the analysis, the relevant practice of the European Court of Human Rights (ECtHR) is summarized, which is gradually adapting to digital realities while preserving the fundamental principles of the ECHR. It is substantiated that existing legal mechanisms, including international ones, are not sufficiently effective in the context of new risks caused by the autonomy, opacity, and potential bias of artificial intelligence technologies. The necessity of combining technical standards with ethical requirements and legal obligations is emphasized. Finally, the need for harmonization of regulatory and legal frameworks is justified, taking into account the dynamics of artificial intelligence development and the priority of protecting human dignity and rights. To this end, specific proposals for amendments to individual articles of the ECHR are developed to improve legal mechanisms for protecting human rights in the context of the widespread use of artificial intelligence technologies.

Keywords: human rights, artificial intelligence, European Convention on Human Rights, rule of law, non-discrimination, privacy, fair trial, automated decisions, ethical standards.

Introduction

In modern conditions, artificial intelligence (AI) technologies have transformed from a scientific abstraction into an everyday reality, rapidly changing the way society, the state, and human interactions function. Algorithmic systems are increasingly being applied in areas that directly affect human rights, such as healthcare, justice, employment, and social security. On the one hand, AI opens up new opportunities for increasing the efficiency of management processes, optimizing public services, and developing innovations. However, serious risks arise related to violations of the right to privacy, non-discrimination, transparency of management decisions, disproportionate surveillance (interference with the right to privacy), and reduced opportunities for challenging such decisions.

Addressing these challenges is particularly important in the context of the ECHR, which serves as the main international instrument establishing human rights protection standards in the European space. The emergence of systems capable of independently making decisions or significantly influencing their adoption requires a careful rethinking of how traditional legal principles, justice, transparency, impartiality, and accountability—can be implemented in the digital age. Therefore, the relevance of this research lies in the need for a systematic analysis of

the legal consequences of AI application from the perspective of ECHR compliance, as well as the development of appropriate approaches to regulatory frameworks that will ensure a balance between technological progress and fundamental human rights.

Research Aim

The purpose of this article is to comprehensively examine the challenges that AI technologies may pose to the human rights protection system within the framework of the ECHR, and to substantiate approaches to their effective regulatory settlement. To achieve this goal, the article sets forth the following tasks: 1) to define the main concepts related to AI technologies and their regulatory definition in the context of the ECHR; 2) to analyze fundamental human rights guaranteed by the ECHR that are affected by the use of AI technologies; 3) to explore the ECtHR's practice regarding the application of the ECHR in cases related to technologies, which allows for assessing the potential for adapting existing standards to the digital age; 4) to identify the main gaps and risks in AI regulation that may hinder effective human rights protection; 5) to formulate proposals for supplementing the ECHR to improve the regulation of individual human rights.

State of Research

The problematic aspects of AI technologies' impact on human rights and the adaptation of human rights protection mechanisms to the challenges of widespread digitalization have been the subject of research by many scholars. Among the academics who have devoted their research to this issue are Yu. Vyshnevskaya, Yu. Volkova, A. Hachkevych, Yu. Kamardina, S. Korneyeva, O. Kotukha, O. Turuta, and others. Attention should also be paid to some studies by foreign scholars, including P. Beckers, H. Weerts, R. Xenidis, L. Stefani, and others. Some aspects of this problem have also been studied by the author, Inna Bernaziuk .

An analysis of existing scientific works on the impact of AI technologies on human rights indicates that most scholars agree that human rights protection mechanisms, in the context of the widespread implementation of AI technologies into public administration and other areas of social relations, require rethinking and improvement. Specifically, Yu. Kovalenko and M. Voinov explored the interconnection between AI, human rights, and national security, proposing guidelines and limitations for AI use in the defense sector, with due regard for human rights. O.V. Turuta and O.P. Turuta argued that the rapid development of technologies could negatively affect human rights, seeing risks to fundamental human rights in the unpredictability of the consequences of applying such new technology. Similarly, A. Ye. Shevchenko, S. V. Kudin, and O. I. Kosilova, in their study of the impact of AI technologies on the realization of human and citizen rights and freedoms in Ukraine, concluded that this impact is particularly noticeable concerning the right to privacy, freedom of expression, and a fair trial.

Some foreign scholars, such as M. Ho-Dac, also question the effectiveness of current approaches to regulating AI technology use in European countries and propose strategic alliances to ensure human rights in the process of standardizing new technologies/

Regarding the protection of the right to privacy in the process of AI technology implementation, it is necessary to refer to the research of some scholars. Specifically, H. Weerts, R. Xenidis, et al. analyzed the correlation between concepts of algorithmic unfairness and EU legal norms on non-discrimination. The authors concluded that there is a discrepancy between technical metrics of fairness and legal standards, emphasizing that the law cannot be reduced to a simple decision tree.

The international legal regulation of AI technology use and its compliance with human rights standards, particularly the new 2024 Council of Europe Convention and its impact on Ukrainian national legislation, is the subject of a scientific article by Yu. V. Kamardina, S. O. Poliariush-Safronenko, and Yu. V. Vyshnevskaya. Similarly, Laulhé Shaelou, S., and Y. Razmetaeva analyzed the challenges that AI technologies pose to fundamental human rights in Europe, emphasizing the need to form a digital legal order that combines the principles of the rule of law and European values.

Discussion

To outline ways to reduce the negative impact of AI technologies on fundamental human rights, particularly those enshrined in the ECHR, it is important to define the main concepts related to AI technologies. First and foremost, it is

crucial to understand the meaning of the concept of "artificial intelligence," which can form the basis for regulatory frameworks governing the use of relevant technology. Currently, this concept is defined in several international acts.

In the EU AI Act (2024), the term "artificial intelligence system" is used, defined as a machine-based system designed to operate with varying levels of autonomy, that can demonstrate adaptiveness after deployment, and that, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

In UNESCO's Recommendation on the Ethics of AI (2021), this concept is considered as engineering systems that generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments, for a given set of objectives, by using machine perception, comprehension, planning, learning, and action.

The concept of "artificial intelligence" is also mentioned in the OECD AI Principles (2019), which state that these are machine systems capable of influencing environments by making autonomous decisions, analyzing data, or interacting with humans/other systems.

A comparative analysis of these definitions of "artificial intelligence" suggests that, in a regulatory aspect, AI is characterized by the following criteria: 1) Autonomy: Defined as a system that can act independently (in various forms: from partial to complete). 2) Purposefulness: All definitions mention that AI has a purpose or task that is realized through generating decisions, predictions, actions, etc. 3) Ability to analyze and make decisions: The main function that mimics human cognitive abilities. 4) Influence on the environment: Both real (physical) and virtual.

However, despite some unified characteristics, the legal definition of AI remains a subject of scientific debate, as it varies from a narrow to a broad understanding, thereby creating a certain legal uncertainty. Nevertheless, despite this uncertainty, AI technologies are finding increasingly wide application in areas directly related to human rights guaranteed by the ECHR, which can negatively impact fundamental human rights, requiring necessary measures from states and interstate associations.

In exploring the possible ways AI technologies affect human rights, the right to respect for private life (Article 8 ECHR) is particularly vulnerable in this regard. As Article 8 ECHR broadly interprets the concept of "private life," including not only the physical and psychological integrity of a person, their identity, the right to image, establishing and developing relationships, but also professional activity and personal data protection, the development of AI thus poses significant threats to the exercise of this right.

One such threat is the uncontrolled and unregulated use of Facial Recognition Technologies (FRT), which are based on the analysis of biometric data for identifying, verifying, or categorizing individuals. Such technologies can constitute a serious interference with an individual's right to respect for private life, as confirmed by ECtHR practice. For example, in the case of *Glukhin v. Russia* (Application No. 11519/20), the ECtHR recognized that an individual has a legitimate expectation of privacy, even when in public places, referring to that person's right to a private social life. The Court referred to FRT in the context of a peaceful protest action, without proper legal regulation and control, as a "highly intrusive" interference with private life, constituting a violation of Article 8 of the Convention (p. 73, 86, 88, 89).

Moreover, since AI technologies are inextricably linked with the processing of large volumes of data, the use of some of these technologies may pose a threat to generally accepted data protection principles in the European community, particularly during their automated processing. These principles, which include lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability, derive from the content of Article 8 ECHR and are detailed in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) and the EU General Data Protection Regulation (GDPR, 2016).

However, the nature of many AI systems, especially those based on machine learning, can contradict the aforementioned principles because: 1) these systems often require vast datasets for effective training, which is inconsistent with the data minimization principle (collecting only data necessary for the stated purpose); 2) the complexity of AI algorithms and their ability to detect non-obvious correlations create a risk of data reuse for purposes incompatible with the initial purpose of collection (violation of the purpose limitation principle); 3) adherence to the transparency principle during data processing by AI systems is also complicated by the inherent opaqueness and inaccessibility of AI algorithms.

The ECtHR's practice concerning mass surveillance and data retention (e.g., *S. and Marper v. the United Kingdom* (Applications No. 30562/04 and 30566/04, p. 66-70) , *Big Brother Watch and others v. the United Kingdom* (Applications No. 58170/13, 62322/14, and 24960/15, p. 325, 345-347) , *Roman Zakharov v. Russia* (Application No. 47143/06, p. 329-333) , etc.) confirms that without adherence to the principle of "quality of law" regarding the regulation of mass surveillance technologies and the limits of such use, the latter cannot be considered lawful. The Court has repeatedly emphasized that the law must be clear, foreseeable, and contain sufficient safeguards against abuse, including independent oversight and effective remedies. These principles are directly applicable to AI systems used for surveillance or analysis of large datasets, even if these systems are developed by private companies but used by the state or at its request.

Another right guaranteed by the ECHR that may be violated during the use of AI technologies is the right to equality and the prohibition of discrimination (Article 14 and Protocol No. 12). One of the greatest risks to the realization of this right is algorithmic bias, which can lead to discriminatory outcomes in the use of AI technologies. The sources of such bias are identified as follows: 1) Biased training data: If the data on which AI is trained reflects existing societal stereotypes, inequalities, or historical discrimination (e.g., in employment, credit, or law enforcement data), the algorithm can "learn" these biases and reproduce them in its decisions. 2) Design flaws: The selection of features, the definition of the target variable, or the method of data labeling can contain hidden biases. 3) Use of proxy variables: Algorithms may use seemingly neutral data (e.g., zip code, purchase history) that strongly correlate with protected characteristics (race, socio-economic status), leading to indirect discrimination.

The ECtHR has repeatedly considered cases of indirect discrimination, including: *D.H. and others v. Czech Republic* (Application No. 57325/00, p. 110-115) (discrimination against Roma children in access to education) and *Biao v. Denmark* (Application No. 38590/10, p. 96-101) (discrimination based on origin in family reunification). In its decisions in these cases, the Court stated that any differential treatment of persons in similar situations requires objective and reasonable justification, and the measures must be proportionate to the legitimate aim pursued. The same approach is fully applicable to algorithmic discrimination when using AI technologies.

The right to a fair trial, guaranteed by Article 6 ECHR, is particularly sensitive concerning the application of AI technologies, especially in justice. This right includes the right to hearing by an independent and impartial tribunal established by law, the presumption of innocence, the right to defense, equality of arms, the right to be informed of charges, and the right to an effective remedy (Article 13). The use of AI in justice and law enforcement poses serious challenges to the guarantees enshrined in Articles 6 and 13 ECHR.

One reason for the risks of violating the right to a fair trial is the opacity of some AI algorithms that may be used in justice. Therefore, if decisions (e.g., on detention, type of punishment) or evidence are based on AI conclusions whose logic cannot be understood and verified, this undermines the right to an effective defense, and the accused is deprived of the opportunity to adequately challenge such conclusions, which violates the principle of equality of arms. In this regard, it is important to emphasize that the EU AI Act sets requirements for transparency of AI algorithms and the interpretability of their results for high-risk systems.

Although most recommendations for the use of AI technologies in justice (including the European Ethical Charter on the Use of AI in Judicial Systems) indicate the permissibility of using AI technologies exclusively as an auxiliary tool, even in this case, there is a risk of "automation bias"—the tendency of people to overly trust machine-generated results, even when contradictory information is available. The "anchoring effect" can also come into play, where an initial assessment provided by AI (e.g., risk of recidivism) disproportionately influences the human's final decision. This calls into question the real independence and impartiality of the judge or other decision-making body, even with the formal presence of a "human-in-the-loop". Given this, the EU AI Act requires ensuring effective human oversight of high-risk systems.

Specifically, the EU AI Act contains a direct prohibition on certain AI practices (Article 5) that are considered contrary to EU values and pose a clear threat to fundamental human rights:

Systems that use subliminal, manipulative, or deceptive techniques to materially distort human behavior, causing significant harm.

Systems that exploit the vulnerabilities of specific groups (due to age, disability, socio-economic status) to distort their behavior, causing significant harm.

Systems that evaluate or classify individuals based on their social behavior or personal characteristics, leading to disadvantageous or unfair treatment, etc.

Certain risks in the use of AI technologies also arise regarding the right guaranteed by Article 10 ECHR, which protects freedom of expression and includes the freedom to hold opinions, receive and impart information and ideas without interference by public authority. Specifically, AI technologies can influence freedom of expression in several aspects. Firstly, as social media platforms increasingly use AI technologies to automatically detect and remove content considered illegal (e.g., hate speech, terrorist content) or violating platform rules, along with a positive effect, there is also a significant risk of over-blocking and erroneous removal of legitimate expressions, including political criticism, satire, art, or journalistic materials. AI algorithms can be inaccurate, biased, or unable to account for the context of the expression. Furthermore, the application of AI technologies in the media space can carry risks of disinformation and manipulation, as AI is sometimes used to create and disseminate disinformation, propaganda, and manipulative content, particularly through deepfakes (realistic fake photos, audio, and video).

The above analysis of possible risks and potential threats to fundamental human rights guaranteed by the ECHR, associated with the use of AI technologies, demonstrates that the effectiveness and safety of such use cannot be achieved solely through technological solutions. Solving this problem requires a comprehensive approach that includes, among other things, regulatory frameworks adequate to modern requirements in this area. In this context, the importance of states' positive obligations increases, meaning that states must not only refrain from violating rights through AI technologies but also actively take measures to protect individuals from risks arising from such technologies, including from the actions of private companies that develop and implement such systems.

Meanwhile, an analysis of ECtHR practice in decisions directly or indirectly related to the application of new technologies in the sphere of human rights realization shows a gradual, though cautious, adaptation of ECHR principles to the challenges posed by the development of AI systems. The Court consistently interprets the content of existing rights, such as the right to privacy (Article 8) and freedom of expression (Article 10), in accordance with new contexts, including the online environment, digital data collection, the use of surveillance systems, etc. At the same time, ECtHR practice is predominantly reactive - which results in the Court lagging behind the rapid pace of technological development. Given this and taking into account existing developments in the field of regulating AI technology use in public administration, there is a need to review how some fundamental human rights are enshrined in the ECHR. To this end, the following changes and additions to the ECHR provisions can be proposed.

Article 1 of the Convention (Obligation to respect human rights) should be supplemented with a new paragraph of the following content: "States Parties undertake to ensure that no digital technology, including artificial intelligence systems, leads to a violation of the rights guaranteed by this Convention. All implementations of such technologies must provide for a prior assessment of their impact on human rights and adherence to the principle of technological neutrality". In justification of this proposal, it can be noted that since digital technologies, particularly those based on AI, increasingly affect the realization of fundamental rights, it is important to place an obligation on states to guarantee human rights in the digital environment. At the same time, it is worth considering that excessive interference in the technological sphere can hinder innovation and lead to increased bureaucracy

Part 1 of Article 6 of the Convention (Right to a fair trial) should be supplemented with a new paragraph of the following content: "In processes where automated or algorithmic decision-making systems are applied, the final decision must be made by an authorized human who bears full responsibility. The parties to the process must be informed about the use of such systems and have the right to challenge them". The necessity of such additions is due to the fact that the automation of some decisions cannot guarantee consideration of certain social, moral, cultural norms, contextualism, or legal intuition. In this regard, the presence of an authorized human in the process of making judicial or administrative decisions ensures accountability and transparency. Meanwhile, it is important to refrain from a complete prohibition of autonomous decision-making at certain stages of judicial or administrative proceedings, as this could slow down judicial proceedings and cause problems in administrative management.

In Article 7 of the Convention (No punishment without law), it is appropriate to clarify in a separate part that: "No person may be punished solely on the basis of an assessment made using artificial intelligence algorithms. Such assessments cannot serve as the sole or decisive basis for criminal liability". This addition guarantees the presumption of innocence and prevents the creation of a "criminal profile" without real actions by the individual. At the same time, complete exclusion of such predictions from law enforcement may harm preventive measures in the security sphere, such as risk management in penitentiary institutions.

To eliminate the risks of excessive interference by AI technologies in private spheres of human life, including uncontrolled surveillance (particularly through facial recognition technology), it can be proposed to supplement Part 1 of Article 8 of the Convention (Right to respect for private and family life) with a new paragraph of the following content: "Everyone has the right to protection from the processing of their personal and biometric data by algorithmic systems without sufficient legal, technical, and procedural safeguards ensuring lawfulness, transparency, data minimization, and the right to an effective legal remedy".

For the protection of the right to freedom of expression in the context of automated moderation, especially on online platforms, Part 2 of Article 10 of the Convention (Freedom of expression) should be supplemented with a provision of the following content: "The use of artificial intelligence systems for systematic, disproportionate, or opaque monitoring or censorship of expressions is prohibited. Any restriction must ensure human oversight, transparency, and the possibility of appeal". However, completely excluding the use of AI technologies in content moderation on the internet is impractical, as in some cases such use may be justified by the need to detect disinformation or hate speech.

To ensure the right to an effective remedy in the context of AI technology use, it is necessary to ensure that the individual understands the logic of the decisions on which the AI system is based. Article 13 of the Convention (Right to an effective remedy) should be supplemented with the following provision: "Everyone has the right to a clear explanation and effective review of decisions made with the use of artificial intelligence systems, with the possibility of appealing to an independent body to verify such decisions". At the same time, concerning the proposed changes, it is important to consider that some systems are inherently non-interpretable (e.g., neural networks), so explanations may be either incomplete or technically complex for the user.

To eliminate algorithmic bias that may arise during the automatic reproduction of certain patterns by AI technologies based on extensive data analysis, particularly bias related to race, gender, age, or place of residence, it can be proposed to supplement Article 14 of the Convention (Prohibition of discrimination) with a new paragraph of the following content: "Any form of discrimination is prohibited, including those arising from algorithmic bias or the use of artificial intelligence systems without proper identification and elimination of discriminatory effects. States Parties are obliged to ensure the auditing of such systems and to guarantee legal mechanisms for appeal".

Article 17 of the Convention (Prohibition of abuse of rights) should be supplemented with a provision stating that: "The use of artificial intelligence technologies to circumvent legal safeguards or the bona fide exercise of rights guaranteed by the Convention is prohibited. In particular, actions aimed at mass surveillance, biased profiling, or manipulation of user behavior shall be qualified as abuse of rights". The introduction of this provision to Article 17 of the Convention reduces the risk of manipulation through AI technologies in the sphere of human rights protection. At the same time, it will be necessary for the ECtHR to properly interpret the concept of "circumventing safeguards" or to provide additional legal clarification and detail of this category

In addition to the proposed amendments and additions to the ECHR, some protocols to the Convention also require transformation. Specifically, to broaden the concept of "property" and consider that digital assets have economic value, establishing control over them is a guarantee of information security and the protection of private property. Therefore, Article 1 of Protocol No. 1 to the Convention (on the protection of property) could be supplemented with provisions of the following content: "Everyone has the right to the protection of digital assets, including personal data and the results of algorithmic processing, according to regulatory regimes that take into account their specificity, economic value, and distinction from traditional property". However, it is important to harmonize the application of the category "data ownership," which will be used in the Convention, with the existing intellectual property regime.

Article 4 of Protocol No. 16 to the Convention (on advisory opinions of the ECtHR) should be supplemented with a norm of the following content: "National courts have the right to request advisory opinions from the ECtHR regarding the application of the Convention to new technologies, including artificial intelligence, algorithmic regulation, and digital rights, to ensure unity and predictability of practice". Such clarifications will ensure the possibility of forming a unified, consistent approach to new types of cases and prevent fragmentation of norm interpretation, although it may lead to some overloading of the ECtHR with advisory requests, especially if there are no clear limits on their content

In the context of the development of AI technologies and their impact on human rights, there may be a need to adopt a separate Protocol to the Convention on the protection of human rights in the context of artificial intelligence use. This additional Protocol should provide for : 1) general principles and guarantees of human rights in the digital environment, including principles of ethical and lawful use of AI technologies in areas that may affect human rights; 2) new human rights in the context of AI technology use, namely: the right to an explanation and review of decisions made with AI ; the right to human participation in the adoption or review of administrative or judicial decisions; the prohibition of algorithmic discrimination ; peculiarities of automated decision-making in the public sector; 3) institutional obligations of states to adopt regulatory legal acts ensuring compliance with human rights in the AI sphere, establish independent bodies for oversight, audit, and investigations in this area; 4) principles of international cooperation and harmonization of standards in the field of AI technology use.

Conclusion

AI technologies have a profound and growing impact on the human rights protection system established by the ECHR. This creates significant challenges, particularly for:

The right to respect for private life (Article 8) due to automated surveillance, biometric identification, and automated behavioral prediction.

The right to freedom of expression (Article 10), especially when facial recognition technology is used without proper regulation and control.

The right to a fair trial (Article 6) due to the use of algorithms for decision-making in judicial or administrative proceedings.

The prohibition of discrimination (Article 14) due to the risk of algorithmic bias that can deepen social inequality.

The existing ECtHR practice in cases related to the application of digital technologies demonstrates an adaptability in interpreting ECHR provisions but confirms that existing legal mechanisms are partially limited in the face of new AI challenges. The Court acts cautiously, leaving room for national regulation. The most significant conclusions in this area, set out in ECtHR judgments, are:

Any interference with private life through secret surveillance must be clearly regulated, provide adequate safeguards, be subject to independent oversight, and be proportionate to the aim pursued (*Roman Zakharov v. Russia*).

High standards of legality, proportionality, and transparency for mass surveillance in the digital age require specific national regulation (*Big Brother Watch v. UK*).

Facial recognition technology without proper legal regulation constitutes a highly intrusive interference with an individual's privacy (*Glukhin v. Russia*).

An analysis of the ECHR provisions and its application practice in the context of AI technologies' development and their implementation in human rights-related areas reveals the following main gaps and risks regarding AI use and, consequently, effective protection of conventional rights: 1) Absence of specialized norms in the ECHR directly addressing AI, necessitating the ECtHR to broadly interpret existing articles. 2) Insufficient transparency and accountability of AI algorithms complicate human rights protection. 3) Lack of control over AI application in the public sector, especially in law enforcement, judiciary, and social protection. 4) Inequality in digital access and risks of algorithmic discrimination. 5) Absence of an effective state policy in digital education, hindering a broad understanding of AI technology functioning principles, including among those who make decisions about their implementation.

To eliminate the identified shortcomings and gaps, it is proposed to introduce a series of amendments to the ECHR provisions and develop a Protocol to the Convention aimed at:

Guaranteeing respect for human rights in the digital environment.

Introducing guarantees for explanation and challenging AI decisions.

Prohibiting algorithmic discrimination and mandating human control over automated decisions in the public sector, as well as enhanced protection for vulnerable groups.

Obligating states to implement legislative regulation of AI use in accordance with human rights standards, ensure effective oversight, audit, and legal protection, and promote digital literacy among the population.

Material files

[Original author file](#)