ISSN 2949-2483

Volume 3 Number 4

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2025

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Volume 3, No. 4
2025
DOI: 10.21202/2949-2483.2025.4
ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL
eISSN 2949-2483
Published since 2023, frequency – 4 issues a year. DOI: 10.21202/2949-2483

Address: 42 Moskovskaya Str., 420111 Kazan, Russian Federation
Tel.: +7 (843) 231-92-90
Fax: +7 (843) 292-61-59
E-mail: lawjournal@ieml.ru
Website: https://www.lawjournal.digital
Telegram: https://t.me/JournalDTL_world
VKontakte: https://vk.com/JournalDTL
Yandex.Dzen: https://dzen.ru/JournalDTL
Odnoklassniki: https://ok.ru/JournalDTL

Founder and publisher of the Journal

Kazan Innovative University named after V. G. Timiryasov. Address: 42 Moskovskaya Str., 420111 Kazan, Republic of Tatarstan, Russian Federation. Tel.: +7 (843) 231-92-90. Fax: +7 (843) 292-61-59. E-mail: info@ieml.ru. Website: https://ieml.ru

Certificate on registering a mass medium: EL no. FS 77-84090 of 21.10.2022, issued by Roskomnadzor.
Territory of distribution: Russian Federation, foreign countries.

Date of signing the issue for publication: 2025, December 20. Hosted on the website https://www.lawjournal.digital: 2025, December 25.

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Volume 3, No. 4
2025
DOI: 10.21202/2949-2483.2025.4
ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL
eISSN 2949-2483

Content

Research article
UDC 34:004:341.4:336.225.692:341.123
EDN: https://elibrary.ru/ftfsob
DOI: https://doi.org/10.21202/jdtl.2025.22

UN Cybercrime Convention: Implementing the Mutual Legal Assistance in the Digital Age

Yassin Abdalla Abdelkarim

Asyut Economic Court, Asyut, Egypt

Keywords

cybercrime,
cyberterrorism,
digital technologies,
extradition,
international cooperation,
international criminal law,
international law,
jurisdiction,
law,
mutual legal assistance

Abstract

Objective: to explore the evolution and comparative effectiveness of mutual legal assistance as a practical alternative to universal jurisdiction in the context of countering transnational cybercrime based on the provisions of the UN Cybercrime Convention.

Methods: the paper employs the method of in-depth legal analysis of international legal tools with an emphasis on the provisions of the United Nations Cybercrime Convention. The author has conducted a comparative legal study of the mechanisms of universal jurisdiction and mutual legal assistance, including the study of historical precedents of the application of universal jurisdiction and the evolution of the mutual legal assistance concept within common law, bilateral and multilateral international agreements. Special attention is paid to the analysis of the Hague Convention on Mutual Legal Assistance as a model for organizing international cooperation. The research relies on doctrinal developments and practical results of the application of the legal mechanisms under consideration in the fight against digital threats.

Results: the analysis demonstrated that, despite the humanitarian potential of universal jurisdiction, which allows national courts to carry out extraterritorial prosecution of serious crimes, its practical application is significantly hampered by opposition from sovereign states and selective law enforcement under political influence. An effective consensual alternative is the mechanism of mutual legal assistance, which promotes international judicial cooperation and ensures coordinated counteraction

to cross-border cybercrime while preserving national sovereignty. The author shows that the UN Cybercrime Convention effectively integrates the mutual legal assistance principles through consultations, coordination of jurisdictions, extradition, and transfer of convicted persons and criminal proceedings.

Scientific novelty: the study offers an innovative approach to analyzing the relationship between traditional and modern international legal mechanisms under the global digitalization. The author substantiates the conceptual position according to which the mutual legal assistance, conditioned by both common law practice and modern contractual initiatives, represents a unique comprehensive toolkit that allows overcoming the systemic limitations of universal jurisdiction in the digital age. The research demonstrated that mutual legal assistance de facto creates a consensual practice of applying universal jurisdiction based on the voluntary consent of states, which qualitatively distinguishes it from traditional approaches. For the first time, the implementation of the mutual legal assistance principles in a specialized international treaty on cybercrime was systematically analyzed.

Practical significance: the results obtained highlight the critical role of mutual legal assistance in strengthening global judicial cooperation and effectively curbing transnational cybercrime. The study demonstrates the practical effectiveness of the UN Cybercrime Convention as an effective international legal tool that ensures a balance between the sovereignty of states and the need for international judicial cooperation.

For citation

Abdelkarim, Ya. A. (2025). UN Cybercrime Convention: Implementing the Mutual Legal Assistance in the Digital Age. *Journal of Digital Technologies and Law, 3*(4), 543–569. https://doi.org/10.21202/jdtl.2025.22

Contents

Introduction

It is a fundamental value of humans to seek global peaceful cohabitation to secure continuing civilizational existence, lest violence prevail and anarchism dominate. To avoid this bleak consequence, the international community manages to utilize cosmopolitan legal tools to enforce justice. In international law, several norms serve to provide global access to justice and enhance the international rule of law. A chief norm is universal jurisdiction, which refers to a state's ability to prosecute core crimes extraterritorially even in the absence of a direct nexus to the criminal act. Domestic courts can prosecute heinous crimes globally to promote access to justice. Despite its humanitarian purposes, universal jurisdiction faces challenging obstacles that hinder its application. Sovereign motivation might drive states to refuse foreign jurisdictions over a crime that occurred within national territory. In addition, selective application under political influence undermines the global trustworthiness of universal jurisdiction.

Thus, justice requirements implied developing a suitable norm to replace universal jurisdiction but, in the same time, achieves its humanitarian ends. To tackle sovereign objections, this norm was established on states' consent. Then, international law introduces the concept of mutual legal assistance (MLA) as a practical alternative of universal jurisdiction. MLA offers a consensual exchange of duties among states to collaborate judicially against international severe crimes. Customary international law includes MLA roots, which were grown up by integrating this concept into bilateral and multilateral treaties. Given its effectiveness against international crimes, international law manages to employ MLA in the digital realm, where crimes' severity still jeopardizes justice.

The openness and borderlessness of cyberspace profile criminal acts committed therein by universalism. In the absence of boundaries, cybercrimes' impacts extend far beyond national borders in the real world. To avoid a legal vacuum in cyberspace,

doctrine and jurisprudence sought to employ traditional universal legal notions against cybercrimes. Nevertheless, the inability to apply universal jurisdiction triggered the need to find an adequate alternative. MLA was introduced to facilitate global judicial cooperation to suppress cybercriminals as the required alternative.

Therefore, the research explores the adoption of MLA in international treaties concerning cybercrime by reviewing its roots and nexus to relevant international law norms, i.e., universal jurisdiction. Then, it sheds light on the UN Convention on Cybercrime as the prominent international legal instrument combating cybercrime, elaborating on how this Convention manifested effective implementation of the MLA norm. Thus, it contributes to knowledge by presenting a comprehensive explorative study revealing the established legal approaches to incorporate MLA in a treaty framework regarding the digital realm.

1. Mutual Legal Assistance and Universal Jurisdiction: Interfering Concepts

Universal jurisdiction and mutual legal assistance (MLA) are critical concepts in addressing cross-border severe crimes. Universal jurisdiction permits domestic courts to prosecute gross crimes extraterritorially. However, its application is often limited by political and legal challenges, as not all countries agree on its scope or implementation. The concept of mutual legal assistance manifests in inter-state cooperation schemes to facilitate the prosecution of cross-border crimes. However, critical procedural and legal challenges frustrate the realization of accurate MLA implementation. This foreword indicates the interfering nexus between both notions.

1.1. Universal jurisdiction in International Law: Status Quo

Abdelkarim (2024) indicates that scholars describe universal jurisdiction as the ability of a state to prosecute international crimes regardless of where they occurred or the nationalities of the involved parties. It is a legal tool to address crimes that threaten global order, such as genocide and war crimes. According to Yee (2011), international jurisprudence laid the foundational logic of universal jurisdiction as the International Court of Justice, in the Barcelona Traction case,[1] indicated the existence of an erga omnes obligation upon states and other members of the international community to impose national jurisdiction whenever a fundamental human right is threatened. Each state is legally interested in utilizing national judicial toolkits to suppress gross human rights violations.

[1] Case concerning the Barcelona Traction, Light and Power Company, Limited, Second Phase, Judgment. ICJ Reports. (1970). 3.

Furthermore, universal jurisdiction is supported by treaties and customary international law, although its interpretation varies. Customary law and international judgments have contributed to its recognition as a principle for prosecuting core international crimes. He adds that universal jurisdiction presents a major evolution in international criminal justice by allowing states and international bodies to prosecute grave crimes regardless of where they occurred or the nationalities involved. This principle curtails the impunity of international criminals and reinforces global justice in the face of severe human rights violations. Notably, as Mung'omba (2022) points out, it does not require a direct connection between the prosecuting body and the location of the crime, which distinguishes it from conventional territorial laws.

Practicing universal jurisdiction against core international crimes fulfills a binding jus cogens obligation—a duty of the international community to safeguard human rights and ensure world peace (Abdelkarim, 2024). This viewpoint is supported by the International Law Commission's stance that protecting fundamental human rights and prohibiting severe crimes such as war crimes, aggression, and slavery creates an international duty to intervene (James et al, 2016; Pielemeier, 2025). In this venue, Hartig (2023) figures out a clear distinction between universal jurisdiction and other related principles in international law. She emphasizes that universal jurisdiction uniquely enables a state to act as an agent of the international community, allowing it to prosecute crimes without requiring any connection between the crime's location and the prosecuting jurisdiction. This differs from cases in which a state prosecutes a foreigner for a crime committed abroad—such prosecutions fall under the principle of representation because the state is acting solely on its behalf rather than on behalf of the international community. Moreover, Hartig (2023) contrasts universal jurisdiction with treaty-based jurisdiction. While treaty-based approaches are bound by the specific terms of the treaty and the processes of domestic ratification, universal jurisdiction stands alone as an independent legal principle. Its legitimacy and applicability are reinforced by international legal precedents dating back to the landmark Nuremberg trials, which helped crystallize universal jurisdiction as a tool for prosecuting international core crimes.

However, Fernandez-Jankov (2025) challenges the traditional notion of state sovereignty by arguing that the domestic implementation of universal jurisdiction is not optional but a fundamental and binding obligation under international law. She emphasizes that universal jurisdiction differs from other jurisdictional bases, such as territoriality, nationality, or the protective principle, because it does not rely on a direct connection between the state and the crime. Instead, it mandates state action against international crimes that violate core peremptory norms (jus cogens), including genocide, torture,

and crimes against humanity. Furthermore, she posits that universal jurisdiction acts as a «conditio sine qua non» for fulfilling international legal obligations. Differently put, every state has a duty to either prosecute or extradite individuals accused of such heinous crimes, regardless of any direct link to its territory. This collective responsibility underscores the idea that these crimes are offenses against the entire international community rather than isolated national issues, thereby reinforcing the rule of law on a global scale. Her perspective ultimately redefines state jurisdiction: while traditional jurisdictional methods allow states a degree of discretion based on territorial or national connections; universal jurisdiction imposes an imperative duty that transcends these limits to ensure that international crimes are subject to accountability worldwide.

Despite universal jurisdiction's humanitarian ends, without a carefully defined framework, universal jurisdiction risks being misused as a political tool (Yee, 2011; Abdelkarim, 2024). When foreign courts intervene in national legal matters, they may essentially become "tyrannical judges" over their own politicians or non-political international criminals, thereby undermining the sovereignty and independence of national judiciaries. Yee (2011) stresses on universal jurisdiction selective application motivated by mere political incentives, relying solely on the concerned state's political strength in the international community. In particular, with the complete absence of a comprehensive treaty on universal jurisdiction organizing its scope and application, undesired sorts of its application prevail, achieving consequences contradicting to universal jurisidiction pure humanitarian ends.

In the same vein, the African Union (AU) has been particularly critical, viewing such practices as a Western tactic to control or subjugate African legal systems.[2] The AU emphasizes that domestic proceedings should be given priority and that international interventions, such as the case against former Sudanese President Omar El-Beshir, violate the principle of complementarity, which reserves international jurisdiction as secondary if national courts have not yet acted. Moreover, African delegates at UN meetings have stressed that the application of universal jurisdiction must take into account the unique characteristics of domestic judicial systems.[3] Requiring the consent of national jurisdictions before foreign proceedings can begin is key to avoiding selective or biased prosecutions.

---

2 African Union Doc PSC.PR/COMM.(DXIX) Communiqué, Peace and Security Council 519th. (2015, June 26). https://clck.ru/3Qfc7s

3 The UNGA Sixth Committee (Legal). (2021, October 22). Concluding Debate on Universal Jurisdiction Principle, Sixth Committee Speakers Wrestle with Challenging Balance between State Sovereignty, Fighting Impunity. (SEVENTY-SIXTH SESSION, 15TH MEETING (AM)), GA/L/3642. https://clck.ru/3QfcA2

Ultimately, misusing universal jurisdiction disrupts the international legal order and strains diplomatic relations, and jeopardizes the effective prosecution of serious crimes by allowing high-ranking offenders to escape justice, thereby fostering a climate of impunity. A conclusion that invites further reflection on maintaining the balance between international justice and national sovereignty, and ensuring that the fight against gross human rights violations does not become entangled in political agendas. Therefore, the utility of universal jurisdiction implies developing a mechanism capable of handling the practical odds of this principle.

1.2. Emergence of Mutual Legal Assistance

1.2.1. What is MLA?

Being practically challenging to utilize universal jurisdiction to prosecute heinous crimes, legal systems adopted a novel notion to facilitate the application of universal jurisdiction. The latter has become a key focus in international legal practice through the mechanism of mutual legal assistance. Mutual Legal Assistance (MLA) is a vital mechanism for international collaboration to combat crime across borders. It enables countries to cooperate in preventing, investigating, and prosecuting criminals who exploit jurisdictional boundaries to evade justice.

According to the European Commission, mutual legal assistance is a cooperative process where countries exchange information and evidence to support criminal investigations across borders (Abdelkarim, 2024). In response to the challenges of universally applying jurisdiction, especially concerns about undermining national judicial independence, states have established multilateral agreements that organize inter-state judicial cooperation. This framework ensures that judicial proceedings initiated via mutual legal assistance occur with the consent and coordination of the involved states parties, thereby preserving the independence and trustworthiness of national judiciaries while still addressing international crimes.

A notable case raising questions on this notion is the Boston College case, which raises significant legal and ethical questions on the MLA notion. This concept invokes inter-state complexities of international cooperation in criminal investigations. In this case, the application of the treaty between the US and the UK, which permits the exchange of evidence, challenges the promise of confidentiality made to interviewees, which was central to the oral history project[4]. Ethically, the case underscores the responsibility of researchers and institutions to protect their participants, especially in sensitive contexts like post-conflict

[4] Harrington, J. (2012). Mutual legal assistance, Boston College, and tales from the Troubles, EJIL TALKS. https://clck.ru/3QfhBd

societies. The breach of confidentiality could deter future participants from engaging in similar projects, potentially stifling efforts to preserve historical narratives. Moreover, it raises questions about the moral obligations of academic institutions when faced with legal demands that conflict with their ethical commitments.

However, international law still lacks a comprehensive approach to interpreting MLA and integrating it into a practical legal framework. A multilateral legal instrument to enhance inter-state cooperation on mutual legal assistance (MLA) and extradition for prosecuting international crimes proves an urgent need.

1.2.2. A Treaty Perspective: the Hague Convention on Mutual Legal Assistance

A key manifestation of MLA is the establishment of Mutual Legal Assistance Treaties (MLATs), which are bilateral or multilateral agreements that foster government-to-government cooperation in criminal investigations and prosecutions (Vũ, 2023). These treaties are crucial for addressing crimes with foreign elements and transnational organized crime. Requests for MLA are typically made by senior officials like Attorney Generals on behalf of law enforcement or prosecuting agencies, ensuring a structured approach to sharing evidence and expertise globally.

De Busser (2017) highlights the long yet underappreciated history of mutual legal assistance (MLA), especially its connection to extradition. The origins of extradition as a form of inter-state cooperation in criminal matters date back to ancient treaties, such as the one between Egyptian Pharaoh Ramses II and Hittite King Hattusili. A key feature of these agreements was reciprocity, reflecting their primary focus on protecting state interests rather than individuals. Another historical aspect of MLA is the use of diplomatic channels for transferring requests, a practice that persists in older agreements. This underscores the state-centered nature of such cooperative mechanisms. Then, after World War II, MLA gained a European centrism due to its adoption by the Council of Europe in 1959. A convention was adopted organizing a European scheme of MLA. On the UN level, MLA was incorporated explicitly in the 2004 UN Convention on Organized Crime[5]. Article 18 addresses states parties to utilize MLA to combat transnational organized crimes because this notion proves effective against cross-border illegal activities. the universal theme of MLA enables it to enhance inter-state endeavors to suppress international crimes, with ultimate compliance with domestic laws.

[5] United Nations Convention against transnational organized crime and the protocols thereto. (2004). UN. https://clck.ru/3QfcGa

The Hague Convention on Mutual Legal Assistance,[6] adopted on 26 May 2023, introduces an exemplary method for organizing universal jurisdiction among states parties. Its preamble asserts that combating impunity for international core crimes is a universal duty, obliging states to unite their legal efforts to ensure that perpetrators do not escape justice (Sadat, 2023). To support this goal, the Convention redefines the notion of «core crimes» so that judicial bodies have a clear, disciplined threshold for applying its mechanisms. A key feature of the Convention is the extension of state jurisdiction over crimes committed abroad when the perpetrator is present within a state's territory (Sadowski, 2025). It establishes a robust multilateral framework that codifies clear obligations to ensure their applicability and efficiency. Such firm, treaty-based obligations are less common in agreements that depend solely on customary international law or loosely structured bilateral treaties. Therefore, the Convention considers respect for the independence of national judiciaries by stipulating state consent to implement the judicial proceedings under the agreement.

A prominent duty under the Convention is the aut dedare aut judicare obligation. This obligation implies that the state where a perpetrator is found must either surrender the case or prosecute the individual under its jurisdiction (as specified in Article 8). This requirement acts as a form of mutual legal assistance, ensuring that states cooperate by transferring cases in a manner that respects each party's judicial independence[7]. To address the practical difficulties posed by cross-border legal proceedings, the Convention utilizes distance video conferencing and telecommunications. This provision ensures that witness testimonies and expert evidence can be effectively collected and heard during trials, even if witnesses are not physically present in the courtroom, thereby enhancing the overall effectiveness of the judicial process (Sadat, 2023). A dual approach that reinforces cooperation between states parties and modernizes trial procedures, ensuring that key evidence is preserved and justice is upheld despite geographical constraints.

However, this provision was initially met with opposition from France and the UK[8]. These states argued that the requirement of the defendant's presence was not

6 Government of the Republic of Slovenia. (2023). The Ljubljana–The Hague Convention on International Cooperation in the Investigation and Prosecution of the Crime of Genocide, Crimes against Humanity, War Crimes and Other International Crime. https://clck.ru/3Qfd7t

7 Pillai, P. (2023, August 4). Symposium on Ljubljana – The Hague Convention on Mutual Legal Assistance: Critical Reflections – Lessons Learned: Civil Society Engagement in Treaty Negotiations. OpinioJuris. https://clck.ru/3QfhHm

8 Government of the Republic of Slovenia. (2023). Final document – English: Mutual Legal Assistance and Extradition Initiative (MLA Initiative). https://clck.ru/3Qfd8n

clearly established in either the treaty or customary international law, and therefore demanded a flexible approach to its application (Sadat, 2023). Ultimately, a consensus was achieved through a reservation-based mechanism that permits states parties to limit the scope of Article 8 under domestic laws (Sadowski, 2025). The Convention promotes international legal cooperation and embeds safeguards that protect national judicial independence while enhancing the global fight against impunity for grave crimes. This development marks a significant step forward in aligning international legal practice with the need for consistent and disciplined application of universal jurisdiction.

Nevertheless, by framing cooperation as a mutual legal assistance obligation, the Convention reinforces a state's commitment to its conventional obligations without undermining domestic judicial processes. Many earlier instruments risked weakening national legal integrity through foreign interventions (Sadowski, 2025). The Convention, by solidifying the principles of mutual assistance and respect for national sovereignty, builds trust among states parties and ensures a coordinated and trusted process in international criminal justice. In this context, Pillai[9] argues that the MLA in the Convention introduces a de facto consensual practice of universal jurisdiction. The concept of legal assistance tackles sovereign opposition to universal jurisdiction since states tend to admit foreign judicial proceedings under a consensual treaty MLA obligation (Sadowski, 2025). A conventional cohesion that enhances universal jurisdiction applicability in international legal practice because of its unified framework, which eliminates logistical and legal obstacles hindering the universal prosecution of gross human rights violations.

In summary, compared to other international legal agreements, whether bilateral mutual legal assistance treaties, regionally focused conventions, or broader instruments like the Rome Statute, the Hague Convention on Mutual Legal Assistance offers a more structured, technologically adaptive, and sovereignty-respecting method for international cooperation. It stands out by codifying obligations explicitly and ensuring that the fight against impunity for severe international crimes is pursued in a manner that upholds both global justice and national judicial independence.

[9] Pillai, P. (2023, August 4). Symposium on Ljubljana – The Hague Convention on Mutual Legal Assistance: Critical Reflections – Lessons Learned: Civil Society Engagement in Treaty Negotiations. OpinioJuris. https://clck.ru/3QfhHm

2. In the UN Cybercrime Convention

2.1. A Brief

After 20 years of debating and negotiating, the United Nations General Assembly has consensually adopted a universal convention on cybercrimes.[10] The treaty aims to strengthen international cooperation in combating cybercrime and sharing electronic evidence for serious crimes. It was the fruit of extensive endeavours started from the UN's resolution 74/247 (2019), which established an open-ended committee to create a global convention on combating the criminal use of information and communication technologies (ICTs), considering existing international and regional efforts. The committee's operational framework in New York and Vienna, starting January 2022, aims to produce a draft convention for the UN General Assembly's seventy-eighth session according to Resolution 75/282 (2021). The proposed United Nations Convention against Cybercrime emphasizes the urgent need for international cooperation to prevent and counter cybercrime, given its adverse economic, social, and legal impacts (Osula, 2015). It will provide tools and a legal framework for tackling cybercrime and facilitate evidence-sharing in electronic forms for various crimes, e.g., money laundering, terrorism, trafficking, corruption, and drug-related offenses.

The Convention was officially adopted on 24 December 2024, reflecting a cosmopolitan consensus on the necessity of gathering states' efforts to combat cybercrimes to secure human communications in cyberspace. As included in its preamble, cyberspace communications technologies have vast potential for societal development and offer opportunities for criminal activities that harm individuals, enterprises, and nations. These technologies have amplified the scale, speed, and scope of crimes such as terrorism, trafficking, smuggling, drug offenses, and cultural property theft. Therefore, to combat cybercrime, the need is immense for global criminal justice policies, including legislation, procedural powers, and international cooperation, under a treaty framework. This includes denying safe havens to cybercriminals through prosecution, enhancing state coordination, and providing technical assistance, particularly to developing countries, to strengthen their frameworks and capacities for preventing, detecting, investigating, and prosecuting cybercrime.

2.2. Absence of Universal Jurisdiction

Article 22 (2) of the Convention explicitly addresses that a state party can impose national jurisdiction under the passive personality perspective. A state party can prosecute perpetrators of cybercrimes extraterritorially if the victim holds its nationality. This reflects

[10] UN General Assembly adopts milestone cybercrime treaty. (2024, December 24). https://clck.ru/3Qfd9n

a limited application of universal jurisdiction because imposing extraterritorial jurisdiction is conditioned by the victim's nationality. It is not absolute for a state party to practice jurisdiction over cybercrime prosecution under the convention despite its universal theme. Moreover, skeptics ignite harsh debates regarding the passive personality approach to sovereignty, due process, and human rights implications.

Scher-Zagier (2024) indicates that Article 22 of the Convention has sparked significant debate due to its jurisdictional provisions, particularly the inclusion of passive personality jurisdiction. According to the aforementioned explanation, this principle permits a state to claim jurisdiction over crimes committed outside national borders if its nationals are harmed. While this approach aims to address the transnational nature of cybercrime, it raises concerns about sovereignty and legal overreach. Critics argue that by adopting this provision, states effectively relinquish their exclusive right to regulate the conduct of their citizens within their territory (Scher-Zagier, 2024). As a result, one state enforces its laws extraterritorially, conflicting with the domestic laws of another state. A bleak scenario of international justice in the digital realm, because jurisdictional conflicts severely jeopardize prosecution endeavours. Nevertheless, supporters present this jurisdiction as a necessary tool to combat cybercrime, which often transcends borders and exploits jurisdictional gaps (Scher-Zagier, 2024). The provision reflects the growing need for international cooperation in addressing crimes that impact individuals and entities across multiple nations. Therefore, he advocates for passive personality jurisdiction as a revolutionalized application of traditional jurisdictional notions adaptable to the specific universal nature of cybercrimes.

Being a crime that transcends national borders and exploits the anonymity inherent to cyberspace, the traditional limits of jurisdiction must yield to a more universal legal mandate to prosecute cybercrime. Kittichaisaree (2017) argues that technical challenges—especially those introduced by cloud computing—complicate the implementation of universal jurisdiction in cyberspace, as multiple states may assert extraterritorial jurisdiction over cloud-based activities. He notes that existing legal instruments permit the prosecution of an unauthorized broadcast originating from a vessel on the high seas, and he extends this reasoning to cover cyber broadcasts by internet platforms such as Facebook[11] and YouTube[12]. Accordingly, states are given a legitimate basis to enforce

[11] The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.

[12] The foreign person owning the YouTube informational resource violates the legislation of the Russian Federation.

their jurisdiction to suppress cybercriminals. Given the rapidly expanding and low-cost nature of cybercriminal activities compared to their severe impacts, Kittichaisaree (2017) concludes that the Budapest Convention on Cybercrime (2014) should be universalized to create a global framework for prosecuting cyber terrorists. Likewise, drawing on the well-established international legal principle of «aut dedere aut judicare» (either extradite or prosecute), Iftikhar (2024) contends that states must take active responsibility for ensuring that cybercriminals do not evade justice. In practice, this means that if a cybercriminal is identified within a state's territory, that state is compelled either to prosecute the individual under its own legal system or to extradite them to a jurisdiction that is both willing and able to try the case. This approach is advanced as a necessary response to the challenges posed by the borderless nature of cyberspace, where traditional mechanisms of jurisdiction prove ineffective (Iftikhar, 2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ Computer Science, 10, e1772. https://doi.org/10.7717/peerj-cs.1772). Universal jurisdiction offers a firm legal groundwork for a cooperative and effective international response against cybercrime, insisting on either prosecuting or extraditing alleged perpetrators, regardless of where in the digital sphere their crimes originated.

Deriving from this logic, passive personality jurisdiction addressed in Article 22 (2) proves insufficient to suppress cybercriminals because it limits national jurisdiction to a prima facie condition: the victim is a national. Thus, the Convention deprives states parties of prosecuting cybercrimes in the absence of this procedural nexus, which hinders global endeavours to realize justice in the digital realm. Because negotiating states strictly advocated for sovereignty, the Convention adopted passive personality as a limited practical alternative to universal jurisdiction. However, as a practical alternative, passive personality could never close the gap instead of universal jurisdiction. Therefore, the Convention integrated the notion of MLA as an obligation upon states parties to ensure universal prosecution of cybercrimes and deprive the perpetrators of havens to impunity.

2.3. MLA in the Convention: Obligatory Duties

Since MLA offers a practical consensual approach to utilize cosmopolitan efforts against transnational crimes, it becomes a popular treaty solution to tackle hardships concerning imposing universal jurisdiction within a conventional framework (Vũ, 2023). States that solidly refuse universal jurisdiction within national territory find it acceptable to collaborate under a conventional MLA clause. Consequently, the Convention adopted MLA in several positions to facilitate judicial proceedings to suppress cybercrimes. The United Nations

Office on Drugs and Crime (UNODC) states that MLA is a mechanism that facilitates international cooperation by enabling countries to share electronic evidence and assist in investigations across borders. This is crucial for addressing the challenges posed by crimes involving cyberspace technologies. Correspondingly, the Convention provides a framework for countries to collaborate effectively while respecting human rights and legal safeguards. It also aims to streamline traditional investigative methods to adapt to the digital environment.

2.3.1. Coordination Through Consultation

Art 22 (5) includes inherent coordination between states parties upon practicing jurisdiction over a single cybercrime. This presents an initial manifestation of MLA by enforcing mutual consultations over jurisdictional issues concerning the prosecution of a cybercrime to prevent jurisdictional conflicts in cyberspace. The consultation clause is a coordination mechanism set out in the Convention to address the challenges posed by cybercrime's transnational nature. By referencing to provisions 1 and 2 of the same article, the text that the Convention establishes a permission for multiple States to claim jurisdiction over a particular cybercrime incident, based on factors, e.g., where the offense was committed, where its effects were felt, or the nationality of either the perpetrator or the victim. The core of the provision is the requirement for the competent authorities to consult with one another to coordinate their actions, which might include sharing information, aligning investigative strategies, and clarifying jurisdictional boundaries.

The clause covers instances where a State Party is either formally notified or becomes unintentionally aware that another State is pursuing legal action for the same conduct. This ensures that states remain vigilant about potential overlaps in their legal proceedings. It seeks to avoid duplication of judicial proceedings because cybercrimes, due to their transnational nature, often span multiple jurisdictions. Without coordination, different states might undertake parallel investigations or prosecutions. This coordinated consultation helps avoid duplication of efforts and minimizes the risk of conflicting legal actions. Moreover, early collaboration in the investigative process, states parties can pool resources and expertise, ensuring a more efficient response to complex, cross-border criminal activities. Furthermore, inter-state coordination contributes to avoiding situations where the rights of those under investigation might be compromised by multiple, potentially overlapping legal actions. It supports a balanced approach where law enforcement efforts do not inadvertently violate due process standards across different jurisdictions.

Thus, when a state party becomes aware that another has initiated judicial proceedings related to the same cybercrime, the coordination clause obliges the involved authorities to engage in consultation. The objective of this coordinated dialogue is to harmonize their actions, ensure an efficient and effective investigation, and ultimately deliver effective justice that respects the legal frameworks of all involved states parties.

2.3.2. International Cooperation Principles

Article 35 of the Convention organizes international cooperation on the collection, preservation, and sharing of electronic evidence for criminal investigations and judicial proceedings related to cybercrime by addressing the governing principles of these processes. This provision applies to electronic evidence collected concerning cybercrimes, including evidence stored on or transmitted through information and communications technology systems, which may be crucial to establishing the commission of criminal conduct in the digital realm.

It aims to facilitate international cooperation on sharing digital evidence by establishing a legal framework for obtaining, preserving, and sharing the evidence. Its design promotes the integrity of the evidence required for a cybercrime investigation while safeguarding the legal rights of those involved. Any request to collect or exchange electronic evidence must comply with domestic law and international obligations, following procedures that ensure the request is lawful, necessary, and proportionate to the crime being investigated. This accords with the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters[13]. Therefore, the evidence acquired according to Article 35 should serve exclusively the criminal investigation or judicial proceedings for which it was requested. This limitation is crucial to protect individuals' rights and to prevent potential misuse of sensitive personal or commercially sensitive information. Recognizing that the collection and sharing of electronic data come with unique technical and legal challenges, Article 35 sets out procedures to maintain a firm chain of custody. Moreover, it ensures that the evidence is gathered, stored, and transmitted in a manner that upholds its authenticity and admissibility in court. This, ultimately, helps prevent evidence abuse or its use in ways that would violate fundamental rights.

To enhance human rights protection, Article 35 establishes an oversight mechanism to surveil the evidence exchange. Judicial or administrative review contributes to preventing abusive procedures and ensuring that the rights protected under domestic

[13] EC. (2018, April 17). COM(2018) 225 final. https://clck.ru/3QfdJS

and international law are not violated during the process of evidence acquisition and sharing.

The significance of Article 35 is grounded in its contribution to enhancing cross-border cooperation by providing a common set of rules and procedures. In addition, Article 35 supports efficient mutual inter-state judicial operations against cybercrime. This cooperation is essential for tackling complex, transnational offenses and for building mutual trust between legal systems that may otherwise have divergent rules regarding evidence and privacy[14]. Moreover, this article seeks to strike a balance between empowering law enforcement to combat cybercrime and ensuring that fundamental rights are protected. Consequently, it promotes legal certainty since it offers obvious rules on the collection and exchange of electronic evidence. This certainty prevents potential conflicts of law or abuses that might otherwise arise when digital data crosses international borders (Iftikhar, 2024).

2.3.2.1. Unified Extradition Framework

Extraditing suspects of cybercrimes proves a complicated, conflicting legal issue because of the specific transnational nature of these crimes. A single cybercrime can involve several jurisdictions. Therefore, Article 37 of the Convention provides a detailed legal framework of MLA concerning the extradition of cybercriminals. The article applies to cybercrime offenses defined exclusively in the Convention when the suspect is present in the requested state's territory. Extradition is allowed solely if the alleged offense is punishable under the laws of both the requesting and requested states. For cases where extradition is sought to enforce a final sentence, the requested State may proceed under its domestic law. A state party may, if permitted by domestic laws, extradite for offenses established by the Convention even if those offenses are not punishable under its national law. In cases where an extradition request covers several offenses, with at least one being extraditable and others not strictly so but related, the entire request may be processed under the provisions of this article. The Convention adopted a broadening approach to extradite cybercriminals because extradition presents an effective toolkit to cut off serious perpetrators and defend the international community (Ochi, 2024). Moreover, this approach complies with the flexibility required to maintain an effective standard of MLA (Abdelkarim, 2024) under the conventional obligation to aut dedare aut

[14] Pillai, P. (2023, August 4). Symposium on Ljubljana – The Hague Convention on Mutual Legal Assistance: Critical Reflections – Lessons Learned: Civil Society Engagement in Treaty Negotiations. OpinioJuris. https://clck.ru/3QfhHm

judicare of cybercriminals. Extradition in this context gains priority because it suppresses a severe criminal activity.

Imposing a legitimating shield on the extradition framework, the Convention submits extradition requests to the domestic laws or applicable treaties of the requested state, including conditions related to minimum penalties and grounds for refusal. States are encouraged to expedite procedures, simplify evidentiary requirements, and—where necessary in urgent cases—take provisional measures, such as temporary custody via available channels like INTERPOL, to ensure the suspect's presence at extradition proceedings. Furthermore, if a suspect is a national, the requested state must forward the matter for prosecution, or consider alternative measures such as conditional extradition, while ensuring the suspect's fair treatment and protecting their rights. Most prominently, extradition cannot be granted on discriminatory grounds, e.g., due to race, religion, etc., or solely refused due to fiscal aspects; any refusal must be accompanied by consultation and a clear communication of reasons according to the basic rules of extradition in international law (Ochi, 2024). Last, states parties must designate an authority for extradition matters to maintain an up-to-date global register, and states should push forward to enhance extradition frameworks through bilateral or multilateral agreements. States then would close the gap created in legal practice regarding extradition by the absence of a global comprehensive convention (van der Wilt, 2018; Tosza, 2024). Needless to say, the extension of this legal vacuum to cyberspace offers perpetrators a sally port to enhance their impunity and evade justice. In addition, this supplemental role of bilateral agreements converges with Article 28 of the European Convention on Extradition,[15] which encourages states parties to limit their bilateral agreements to achieve the purposes and objectives of this regional agreement.

2.3.2.2. Inter-State Party Transfer of Sentenced Criminals

Article 38 of the UN Cybercrime Convention establishes an optional mechanism for states parties to cooperate by transferring convicted individuals, thereby they can complete their sentences in another country. The transfer scheme proves advantageous to the sentenced person since transferring to their home territory, or another admissible jurisdiction, improves the comfort and support systems available to the sentenced person, including access to family, community, and familiar legal processes. For the states parties, this mechanism fosters closer inter-state cooperation, potentially easing administrative burdens and reinforcing mutual trust in handling persons convicted of cybercrime-related offenses.

[15] ETS 24 – Extradition. (1957, December 13). https://clck.ru/3QfdLf

Under Article 38, states parties are encouraged to conclude bilateral or multilateral agreements or arrangements to enable the transfer of persons who have been sentenced to imprisonment or another form of deprivation of liberty for cybercrime-related offenses, allowing them to serve the remainder of their sentence in another country's territory. The transfer should be done in compliance with the fundamental legal instruments on human rights (Ochi, 2024). This provision ensures that any transfer respects human rights standards and that the treatment of the person remains in line with fundamental legal and ethical norms.

The provision enhances the legitimacy of the transfer as it demands that states parties consider several critical factors when opting for a transfer. 1. Consent: Ensuring that the person concerned agrees to the transfer. 2. Rehabilitation: Considering whether the transfer might benefit the individual's rehabilitation process. 3. Reintegration: Assessing if serving the sentence in a familiar environment would facilitate the eventual reintegration of the individual into society.

In essence, Article 38 offers a flexible, rights-respecting framework for permitting sentenced individuals to serve their sentences in a territory where they have stronger ties or better rehabilitation prospects. It recognizes that, beyond punishment, factors such as consent, rehabilitation, and reintegration are crucial for the fair and effective application of justice in cybercrime cases.

2.3.2.3. Transfer of Criminal Proceedings

Article 39 of the Convention facilitates international judicial cooperation since it permits states parties to transfer criminal proceedings related to offenses under the Convention. Its primary purpose is to enhance the efficiency and effectiveness of transnational cybercrime prosecutions through a more concentrated and coherent process. Cybercrime investigations frequently span multiple jurisdictions, which can lead to fragmented and inefficient legal proceedings. Thus, Article 39 encourages the parties to consider transferring the criminal prosecution of an offense to one jurisdiction when it is in the interests of the proper administration of justice. The idea is to concentrate prosecution efforts in a single, centralized forum, thereby reducing duplication, minimizing conflicting procedures, and ultimately streamlining the entire judicial process.

Indeed, concentrating proceedings in a single jurisdiction improves coordination between investigative agencies and ensures that crucial evidence is managed effectively. This consolidation offers an organized approach to complex cases, which is particularly valuable when technical evidence, digital data, or multiple international elements are involved. Since states traditionally condition the transfer of criminal proceedings on

the existence of a bilateral or multilateral treaty governing such transfers, Article 39(2) permits states parties to request transfer from another state with which no treaty exists, depending solely on the Convention as the legal basis for that transfer. Furthermore, this provision ensures that a lack of a specific treaty does not become an obstacle to international cooperation. By allowing the Convention to serve as a legal foundation for transferring proceedings, it supports seamless judicial collaboration (de Jonge, 2020), in particular in urgent or complex cybercrime cases where traditional treaty frameworks might be lacking or insufficient. In addition, practical odds contribute to the transfer failure between different jurisdictions because of alien elements the transferred cases include, inter alia, logistical delays and technical shortcomings (de Jonge, 2020). He addresses the European Convention on the Transfer of Proceedings in Criminal Matters[16] as the regional legal ground of criminal proceedings transfer, asserting that open-borders spheres imply a unified consensual legal framework governing the transfer process. The openness of cyberspace justifies adopting this scheme in the Convention to facilitate cybercriminals' prosecution and trying. Therefore, he advocates that cyberspace has added a locus delicti ground for human interactions on the Internet. Its universality facilitates achieving criminal purposes transnationally, which grants the criminal proceedings transfer a cosmopolitan perspective.

Thus, Article 39 enhances judicial efficiency by authorizing the transfer of proceedings to prevent the pitfalls of jurisdictional fragmentation. This creates clearer evidentiary chains, a more straightforward application of the law, and a reduction in procedural delays that might otherwise jeopardize successful prosecutions in cybercrimes.

2.3.2.4. General Principles of MLA

Article 40 of the Convention refers to practical, procedural measures required to promote international cooperation under the notion of MLA in combating cybercrime. In essence, this article is designed to establish the framework for the rapid, secure, and lawful exchange of electronically stored evidence among states parties. In a world where cyber-incidents, and the data or communications that prove them, cross national boundaries, Article 40 sets out the obligations of participating states to provide assistance when one state needs evidence from another for criminal investigations or prosecutions. It recognizes that effective investigations of cybercrime depend on the ability to obtain, preserve, and share electronic evidence without undue delay (De Busser, 2017; Kerttunen & Rantala, 2022), demanding states parties to implement the necessary technical and legislative measures

[16] Council of Europe. (1972, May 15). ETS No. 73. https://clck.ru/3QfdV3

that ensure a rapid and secure processing of evidence requests. Therefore, it codifies states' responses to requests for digital evidence from one another, thereby strengthening the overall international legal framework, creating a legal foundation for MLA.

While the article obliges states to cooperate, it underscores the importance of respecting national legal systems and sovereign decision-making. Differently put, although a state must assist a foreign authority's request for evidence, the process must comply with domestic laws. States retain control over the evidence located within their territory; any cross-border sharing must be done with due regard for constitutional guarantees and the rule of law, which presents a balancing scheme between MLA and national sovereignty[17] (Abdelkarim, 2024). Indeed, the Convention approach herein promotes trust among states parties because assuring a clear process that comply with national laws and protect human rights encourages them to share sensitive evidence.

An essential aspect of Article 40 is its built-in respect for fundamental rights. As states parties collaborate to exchange electronic evidence, they should avert undermining human rights, particularly with respect to privacy and data protection. Hence, the article requires that any measures to collect, transmit, or use such evidence be consistent with a state's international human rights obligations. This balance is critical for ensuring that the fight against cybercrime does not undermine individual liberties.

Cybercriminals benefit from the borderless nature of digital networks. Then, when malicious actors leave traces of their activities spread over several jurisdictions, no single country's investigation tools prove sufficient to combat them. Thus, to make practical cooperation feasible, Article 40 calls for the establishment of ad hoc administrative and technical channels. This may include designating national points of contact or creating secure systems for the exchange of electronic evidence to reduce delays and prevent the bureaucratic obstacles that could otherwise stymie timely investigations into cyber-offences.

To sum up, Article 40 is pivotal because of its contribution to bridging the practical gap between different legal systems and technological realities. It provides a mechanism for states to collectively and effectively pursue cybercriminals, while also setting guardrails that ensure cooperation does not undermine legal or human rights standards. However, its actual utilization relies crucially on national adaptations because states parties will incorporate Article 40 into domestic legislation via approaches reflecting local

[17] Pillai, P. (2023, August 4). Symposium on Ljubljana – The Hague Convention on Mutual Legal Assistance: Critical Reflections – Lessons Learned: Civil Society Engagement in Treaty Negotiations. OpinioJuris. https://clck.ru/3QfhHm

legal traditions. Consequently, implementing convenant obligations might vary between states parties. Therefore, a harmonizing body should take over the dillema and introduce harmonized implemetaion schemes adaptable to states parties' jurisdictions.

Conclusions

Despite being a solid norm in international law, universal jurisdiction still challenging legal and practical odds that hinder its accurate utilization. The state-of-the-art reveals a widespread official refusal to submitting a national crime to foreign jurisdictions, leading to the creation of MLA. This norm was consensually introduced to international legal practice to cure deficiences resulting from universal jurisdiction inabilities. MLA manifests a universal admissible form of inter-state legal cooperation aiming to suppress severe criminals. In particular, the notion proves appropriate to combat serious transnational crimes because of its global consensus.

The research proves that the MLA effectiveness to combat international core crimes has motivated international organizations and jurists to adopt it under a convenant framework to combat cybercrimes. The latter exploit the vague and borderless nature of cyberspace, creating serious transnational criminal activities. Therefore, MLA presents an appropriate solution to be adopted within an international treaty on cybercrime, i.e., the UN Cybercrime Convention, due to proving advantageous as a practical alternative to universal jurisdiction. As revealed by the research, MLA obligations' adaptability to national juridical backgrounds enhances its adoption by the Convention to combat cybercrime.

References

Abdelkarim, Y. A. (2024). A Multi-Dimensional Approach to Impose Universal Jurisdiction in International Legal Practice. *International Journal of Law in Changing World*, *3*(1), 20–32. https://doi.org/10.54934/ijlcw.v3i1.87

De Busser, E. (2017). The Digital Unfitness of Mutual Legal Assistance. *Security and Human Rights*, *28*, 161–179. https://doi.org/10.1163/18750230-02801008

de Jonge, B. (2020). Transfer of criminal proceedings: from stumbling block to cornerstone of cooperation in criminal matters in the EU. *ERA Forum*, *21*, 449–464. https://doi.org/10.1007/s12027-020-00616-8

Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science*, *10*, e1772. https://doi.org/10.7717/peerj-cs.1772

Fernandez-Jankov, F. F. (2025). Universal jurisdiction ensuring the rule of law in international criminal proceedings. *Strani Pravni Život*, *LXIX*(4). https://doi.org/10.56461/SPZ_24405KJ

Hartig, A. (2023). *Making Aggression a Crime Under Domestic Law: On the Legislative Implementation of Article 8bis of the ICC Statute*. TMC Asser Press. https://doi.org/10.1007/978-94-6265-591-1

James, J. I., Gladyshev, P., & Zhu, Y. (2016). A survey of mutual legal assistance involving digital evidence. *International Journal of Law and Information Technology*, *24*(3), 237–265. https://doi.org/10.1093/ijlit/eaw008

Kerttunen, M., & Rantala, T. (2022). Digital evidence in comparative criminal procedure: International cooperation and mutual legal assistance. *Transnational Criminal Law Review*, *4*(1), 55–78.

Kittichaisaree, K. (2017). *Public International Law of Cyberspace*. Springer International Publishing.

Mung'omba, I. (2022). Universal Jurisdiction as a Tool in Promoting Accountability for International Crimes in Africa: Exploring the Significance of Hissene Habre's Conviction. In E. C. Lubaale, & N. Dyani-Mhango (Eds.), *National Accountability for International Crimes in Africa*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-88044-6

Ochi, M. (2024). *The Premises of International Criminal Procedure: Identifying the Principles in International Collaboration*. Shinzansha and Springer Nature Singapore Ltd. https://doi.org/10.1007/978-981-97-6786-1

Osula, A.-M. (2015). Mutual legal assistance & other mechanisms for access to extraterritorial evidence: A study on prospects and challenges in the digital age. *Masaryk University Journal of Law and Technology*, *9*(1), 43–63. https://doi.org/10.5817/MUJLT2015-1-4

Pielemeier, J. (2025). Mutual legal assistance under the UN cybercrime convention: Continuity and change in international cooperation against cybercrime. *International and Comparative Law Quarterly*, *74*(2), 389–416.

Sadat, L. N. (2023). Understanding the New Convention on Mutual Legal Assistance for International Atrocity Crimes. *ASIL Insights*, *27*(12).

Sadowski, M. M. (2025). The Ljubljana – The Hague Convention: A Treaty for the Globalised and Interconnected World? Perspectives from a Legal Semiotics Analysis. *International Journal for the Semiotics of Law*, *38*, 1763–1780. https://doi.org/10.1007/s11196-025-10267-y

Scher-Zagier, E. (2024). *The New UN Cybercrime Treaty Is a Bigger Deal Than Even Its Critics Realize*. Lawfare.

Tosza, S. (2024). Cross-border access to electronic evidence in criminal matters: Between mutual legal assistance and new cooperation instruments. *New Journal of European Criminal Law*, *15*(3), 251–272. https://doi.org/10.1177/20322844241258649

van der Wilt, H. (2018). Extradition and Mutual Legal Assistance in the Draft Convention on Crimes Against Humanity. *Journal of International Criminal Justice*, *16*(4), 795–812. https://doi.org/10.1093/jicj/mqy037

Vũ, H. A. (2023). Practices of Mutual Legal Assistance in Criminal Matters between Vietnam and Southeast Asia Countries. *International Journal of Criminal Justice Science*, *18*(1), 64–78.

Yee, S. (2011). Universal Jurisdiction: Concept, Logic, and Reality. *Chinese Journal of International Law*, *10*(3), 503–530. https://doi.org/10.1093/chinesejil/jmr041

Author information

Yassin A. Abdelkarim – LLM (Master of Laws), Judge, Asyut Economic Court, Founder of Cyber Jurisprudence International Initiative (CyJurII)
Address: Kornish Al Nile (Al Thawra), Asyut 2, Assiut Governorate 2090281, Egypt
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=59725007500
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JPW-9781-2023
Google Scholar ID: https://scholar.google.com/citations?user=kPFaAC0AAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 8, 2025
Date of approval – May 24, 2025
Date of acceptance – December 20, 2025
Date of online placement – December 25, 2025

Научная статья
УДК 34:004:341.4:336.225.692:341.123
EDN: https://elibrary.ru/ftfsob
DOI: https://doi.org/10.21202/jdtl.2025.22

Конвенция Организации Объединенных Наций против киберпреступности: имплементация концепции взаимной правовой помощи в цифровую эпоху

Яссин Абдалла Абделькарим

Экономический суд г. Асьют, Асьют, Египет

Ключевые слова

взаимная правовая помощь,
киберпреступность,
кибертерроризм,
международное право,
международное сотрудничество,
международное уголовное право,
право,
цифровые технологии,
экстрадиция,
юрисдикция

Аннотация

Цель: исследовать эволюцию и сравнительную эффективность взаимной правовой помощи как практической альтернативы универсальной юрисдикции в контексте противодействия транснациональной киберпреступности на основе положений Конвенции Организации Объединенных Наций против киберпреступности.

Методы: в работе применен метод углубленного юридического анализа международных правовых инструментов с акцентом на нормативных положениях Конвенции Организации Объединенных Наций против киберпреступности. Автором проведено сравнительно-правовое исследование механизмов универсальной юрисдикции и взаимной правовой помощи, включающее изучение исторических прецедентов применения универсальной юрисдикции и эволюции концепции взаимной правовой помощи в рамках общего права, двусторонних и многосторонних международных соглашений. Особое внимание уделено анализу Гаагской конвенции о взаимной правовой помощи как образцовой модели организации международного сотрудничества. Исследование опирается на доктринальные разработки и практические результаты применения рассматриваемых правовых механизмов в борьбе с цифровыми угрозами.

Результаты: проведенный анализ продемонстрировал, что, несмотря на гуманитарный потенциал универсальной юрисдикции, позволяющей национальным судам осуществлять экстерриториальное преследование тяжких преступлений, ее практическое применение существенно затруднено вследствие противодействия со стороны суверенных государств и избирательного правоприменения под политическим влиянием. Эффективной консенсусной альтернативой

выступает механизм взаимной правовой помощи, способствующий международному сотрудничеству судебных систем и обеспечивающий координированное противодействие трансграничной киберпреступности при сохранении национального суверенитета. Установлено, что Конвенция Организации Объединенных Наций против киберпреступности эффективно интегрирует принципы взаимной правовой помощи через механизмы консультаций, координации юрисдикций, экстрадиции, передачи осужденных и уголовного производства.

Научная новизна: исследование предлагает новаторский подход к анализу соотношения традиционных и современных международно-правовых механизмов в условиях цифровизации глобального пространства. Автором обоснована концептуальная позиция, согласно которой эволюция взаимной правовой помощи, обусловленная как практикой общего права, так и современными договорными инициативами, представляет собой уникальный комплексный инструментарий, позволяющий преодолеть системные ограничения универсальной юрисдикции в эпоху цифровых технологий. Продемонстрировано, что взаимная правовая помощь де-факто создает консенсусную практику применения универсальной юрисдикции, основанную на добровольном согласии государств, что качественно отличает ее от традиционных подходов. Впервые проведен системный анализ имплементации принципов взаимной правовой помощи в специализированном международном договоре по киберпреступности.

Практическая значимость: полученные результаты подчеркивают критическую роль взаимной правовой помощи в укреплении глобального сотрудничества судебных органов и эффективном пресечении транснациональной киберпреступной деятельности. Исследование демонстрирует практическую эффективность Конвенции Организации Объединенных Наций против киберпреступности как действенного международно-правового инструмента, обеспечивающего баланс между суверенитетом государств и необходимостью международного судебного сотрудничества.

Для цитирования

Абделькарим, Я. А. (2025). Конвенция Организации Объединенных Наций против киберпреступности: имплементация концепции взаимной правовой помощи в цифровую эпоху. *Journal of Digital Technologies and Law*, *3*(4), 543–569. https://doi.org/10.21202/jdtl.2025.22

Список литературы

Abdelkarim, Y. A. (2024). A Multi-Dimensional Approach to Impose Universal Jurisdiction in International Legal Practice. *International Journal of Law in Changing World*, *3*(1), 20–32. https://doi.org/10.54934/ijlcw.v3i1.87

De Busser, E. (2017). The Digital Unfitness of Mutual Legal Assistance. *Security and Human Rights*, *28*, 161–179. https://doi.org/10.1163/18750230-02801008

de Jonge, B. (2020). Transfer of criminal proceedings: from stumbling block to cornerstone of cooperation in criminal matters in the EU. *ERA Forum*, *21*, 449–464. https://doi.org/10.1007/s12027-020-00616-8

Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science*, *10*, e1772. https://doi.org/10.7717/peerj-cs.1772

Fernandez-Jankov, F. F. (2025). Universal jurisdiction ensuring the rule of law in international criminal proceedings. *Strani Pravni Život*, *LXIX*(4). https://doi.org/10.56461/SPZ_24405KJ

Hartig, A. (2023). *Making Aggression a Crime Under Domestic Law: On the Legislative Implementation of Article 8bis of the ICC Statute*. TMC Asser Press. https://doi.org/10.1007/978-94-6265-591-1

James, J. I., Gladyshev, P., & Zhu, Y. (2016). A survey of mutual legal assistance involving digital evidence. *International Journal of Law and Information Technology*, *24*(3), 237–265. https://doi.org/10.1093/ijlit/eaw008

Kerttunen, M., & Rantala, T. (2022). Digital evidence in comparative criminal procedure: International cooperation and mutual legal assistance. *Transnational Criminal Law Review*, *4*(1), 55–78.

Kittichaisaree, K. (2017). *Public International Law of Cyberspace*. Springer International Publishing.

Mung'omba, I. (2022). Universal Jurisdiction as a Tool in Promoting Accountability for International Crimes in Africa: Exploring the Significance of Hissene Habre's Conviction. In E. C. Lubaale, & N. Dyani-Mhango (Eds.), *National Accountability for International Crimes in Africa*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-88044-6

Ochi, M. (2024). *The Premises of International Criminal Procedure: Identifying the Principles in International Collaboration*. Shinzansha and Springer Nature Singapore Ltd. https://doi.org/10.1007/978-981-97-6786-1

Osula, A.-M. (2015). Mutual legal assistance & other mechanisms for access to extraterritorial evidence: A study on prospects and challenges in the digital age. *Masaryk University Journal of Law and Technology*, *9*(1), 43–63. https://doi.org/10.5817/MUJLT2015-1-4

Pielemeier, J. (2025). Mutual legal assistance under the UN cybercrime convention: Continuity and change in international cooperation against cybercrime. *International and Comparative Law Quarterly*, *74*(2), 389–416.

Sadat, L. N. (2023). Understanding the New Convention on Mutual Legal Assistance for International Atrocity Crimes. *ASIL Insights*, *27*(12).

Sadowski, M. M. (2025). The Ljubljana – The Hague Convention: A Treaty for the Globalised and Interconnected World? Perspectives from a Legal Semiotics Analysis. *International Journal for the Semiotics of Law*, *38*, 1763–1780. https://doi.org/10.1007/s11196-025-10267-y

Scher-Zagier, E. (2024). *The New UN Cybercrime Treaty Is a Bigger Deal Than Even Its Critics Realize*. Lawfare.

Tosza, S. (2024). Cross-border access to electronic evidence in criminal matters: Between mutual legal assistance and new cooperation instruments. *New Journal of European Criminal Law*, *15*(3), 251–272. https://doi.org/10.1177/20322844241258649

van der Wilt, H. (2018). Extradition and Mutual Legal Assistance in the Draft Convention on Crimes Against Humanity. *Journal of International Criminal Justice*, *16*(4), 795–812. https://doi.org/10.1093/jicj/mqy037

Vũ, H. A. (2023). Practices of Mutual Legal Assistance in Criminal Matters between Vietnam and Southeast Asia Countries. *International Journal of Criminal Justice Science*, *18*(1), 64–78.

Yee, S. (2011). Universal Jurisdiction: Concept, Logic, and Reality. *Chinese Journal of International Law*, *10*(3), 503–530. https://doi.org/10.1093/chinesejil/jmr041

Сведения об авторе

Абделькарим Яссин Абдалла – магистр права, судья, Экономический суд г. Асьют, основатель международной программы киберюриспруденции (CyJurII)
Адрес: 2090281, Египет, административный округ Асьют, г. Асьют, Корниш аль-Нил (аль-Тавра), Асьют 2
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=59725007500
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JPW-9781-2023
Google Scholar ID: https://scholar.google.com/citations?user=kPFaAC0AAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 8 мая 2025 г.
Дата одобрения после рецензирования – 24 мая 2025 г.
Дата принятия к опубликованию – 20 декабря 2025 г.
Дата онлайн-размещения – 25 декабря 2025 г.

Research article
UDC 34:004:343.213.3:343.232:343.235.4
EDN: https://elibrary.ru/rowsaq
DOI: https://doi.org/10.21202/jdtl.2025.23

Multifactor Model of Jurisdiction: Reviewing Locus Delicti in a Decentralized Metaverse

Murad M. Madzhumaev

Peoples' Friendship University of Russia named after Patrice Lumumba, Moscow, Russia

Keywords

augmented reality,
avatar,
crime,
crime scene,
criminal law,
digital technologies,
jurisdiction,
law,
metaverse,
virtual reality

Abstract

Objective: to critically analyze the possibility of extending the existing spatial criminal law principles to acts committed in the decentralized virtual worlds of the metaverse, and to develop proposals that include updating the approach to establishing jurisdiction over such virtual crimes.

Methods: the methodological basis of the research is a set of general scientific methods and approaches of scientific cognition – dialectical, formal logical (analysis and synthesis, induction and deduction), systematic, as well as private scientific methods – formal legal, legal modeling, interpretation. The study relies on an analysis of judicial practice, foreign legislation, technical features of blockchain technologies and decentralized autonomous organizations, which makes it possible to identify gaps in legal regulation and propose conceptually new solutions for determining the crime scene in a virtual environment.

Results: the study revealed a limited implementation of the current generally accepted principles of determining jurisdiction in relation to virtual crimes that do not have physical coordinates. The proposed multifactorial jurisdiction model redefines the "crime scene" taking into account factors such as the offender's digital identity, the nature and location of digital assets, platform management protocols, and the actual damage caused. Assumingly, the immutable and verifiable nature of blockchain transactions can serve as a legal equivalent of a physical presence to establish personal jurisdiction, allowing criminal prosecution to be initiated even in cases where the actual location of the offender remains unknown.

Scientific novelty: the paper presents an approach that implies the fundamental transformation of reactive, adaptive legal regulation principles into a proactive, comprehensive framework designed specifically for the unique challenges of the metaverse. A paradigm-changing hypothesis was put forward: that a permanent (stable) digital footprint of the offender in virtual spaces can serve to exercise jurisdiction. The model systematically presents the idea of harm as the most important link between virtual offenses and their consequences in the real world.

Practical significance: it is currently impossible to apply legal norms and rules to relations in the metaverse, taking into account their specifics. The main provisions and conclusions of the study can be used to improve the mechanisms of legal regulation of the metaverse and to form international protocols on data exchange and mutual legal assistance for searching and collecting evidence based on blockchain technology. They may help to develop legislative initiatives aimed at creating integrated legal mechanisms that are scalable and resistant to rapid technological changes, characteristic for the digital environment.

For citation

Madzhumaev, M. M. (2025). Multifactor Model of Jurisdiction: Reviewing Locus Delicti in a Decentralized Metaverse. *Journal of Digital Technologies and Law, 3*(4), 570–597. https://doi.org/10.21202/jdtl.2025.23

Contents

Introduction

The emergence of a metaverse, conceptually represented as a network of regulated, permanent, immersive, interactive, and interconnected virtual worlds combining virtual (VR), augmented (AR), and mixed (MR) realities, as well as blockchain technology, poses a serious challenge to established principles of criminal law, especially the definition of the law in space. Historically, state sovereignty and the inalienable right to make and apply laws have been inextricably linked to territoriality, which underlies the Westphalian system of international law and order (Chimni, 2022). It follows from this fundamental principle that the jurisdiction of a state with respect to acts committed on its "physical" territory (on land, in airspace, in internal waters and territorial sea, on the continental shelf and in the exclusive economic zone) is in principle lawful. At the same time, in case of claims with respect to acts committed outside its territory, they are considered illegal (except for the principles of extraterritoriality).

For all its historical roots, such a traditional model (territoriality and generally accepted principles of extraterritoriality) is becoming more and more "artificial" in the digital age. In particular, according to Actor Network theory, objects (artifacts, technical complexes, non-human "agents", algorithms), the so-called actors or actants, are perceived as acting units of public relations (Wei, 2023). Assumingly, such actors (actants) may include digital counterparts of people in the metaverse who are able to interact and influence the virtual network. The main problem lies in the fundamental incompatibility of such a model of jurisdiction, tied to the physical territory of the state, with the limitless, "non-physical" and decentralized architecture of the metaverse. The metaverse is completely devoid of physical coordinates (Brey, 2025).

In this article, we use the terms "locus delicti", "crime scene", and "scene of the incident". Although they are not identical in content, here they will be understood as having the same meaning, except in cases where the opposite is specifically stipulated. Locus delicti (Latin "crime scene") means an area in which there were signs of the crime's objective element. A crime scene is a narrower and more specific concept. This is the main place where the crime was committed, regardless of where the crime's socially dangerous consequences occurred or where information about the crime was discovered.

On the other hand, the scene of the incident is a broader category. It designates a place or territory where there is information related to the event that is being investigated in a criminal procedural manner[1]. This includes not only a specific crime scene, but also any other place where objective consequences of the crime or other traces of criminalistic significance are found.

Determining the location of a crime (locus delicti) is one of the fundamental tasks of criminal law science, since the solution of several fundamental issues depends on it. First, it defines the law applicable to a particular crime, as well as the proper investigative and judicial jurisdiction of the case. The limitation periods of criminal liability are directly related to this, since their establishment depends on the jurisdiction in which the crime was committed. Second, the crime scene serves as a starting point for establishing the constituent elements of the deed and its correct qualification. This, in turn, affects the implementation of "non bis in idem" ("not twice for the same thing") principle and extradition issues.

In the criminal-procedural law, a crime scene is an indispensable landmark for almost all investigative actions. It serves as the main source of evidence, ensuring a proper chain of proving on which their subsequent verification and evaluation depend. In addition, the crime scene is the starting point for finding witnesses, checking alibis, and motivating procedural documents such as the investigator's orders to conduct a search and seizure (or a court decision if a search is conducted in residential premises). All these actions together contribute to building a case that will allow for a reasonable accusation, taking into account the presumption of innocence.

In criminology, a crime scene is a central element that defines the entire investigation process. This is extremely important for inspecting the crime scene, building forensic versions of events and planning further investigative actions. All types of evidence are collected at the crime scene, and their forensic photo and video recording is carried out. In addition, the interaction between investigators (inquirers), employees of operational search units, and, if necessary, authorized representatives of law enforcement agencies of other states is organized. Also, competent persons with special knowledge (specialists and subsequently experts) actively work at the crime scene, which contributes to the effective detection and investigation of crimes.

Determining the location of a crime (locus delicti) is especially important when investigating crimes, the constituent elements of which are fully or partially concentrated in a decentralized virtual space – the metaverse. The total turnover of the global metaverse market is showing rapid growth, estimated as US$ 110.4 billion in 2024 and projected to exceed US$ 4.47 trillion by 2034; it reflects a high cumulative annual growth rate (CAGR)

[1] Bertovskiy, L. V. (ed.). (2021). Criminology: tutorial for Bachelor students (2nd ed., amended and complemented). Moscow: RG-Press.

of 44.8 %[2]. In 2024, the largest contribution was into the hardware segment, which includes advanced headsets and tactile sensors, accounting for 52.8 % of the total market share[3]. The underlying virtual reality (VR) and augmented reality (AR) technologies combined accounted for 34.2 % of the market, forming the basis of immersive digital environments[4].

The user base of the metaverse consists mainly of young people (four out of five users are under the age of 16) and comprises about 700 million active users monthly worldwide[5]. Growth forecasts are quite impressive, with some reports suggesting that by 2030 the number of users will reach 5 billion, taking into account mobile phone users, while more accurate estimations, based on data on VR/AR users, predict a figure closer to 1 billion[6]. This determines the relevance of studying the problem under consideration regarding the definition of locus delicti in deeds committed in the metaverse.

This article examines the fundamental problem of the operation of criminal law in the decentralized virtual environment of the metaverse. First of all, we will analyze the problem of the metaverse criminalization, to use it as the basis for discussing the applicability of traditional legal approaches to it. Further, we will discuss in detail the well-established principles of criminal jurisdiction in space, in particular territorial and extraterritorial approaches and their limitations when applied to a virtual environment. Then we will study the metaverse phenomenon, describing its ontological properties such as immersiveness, synchronicity, stability, compatibility and decentralization, as well as its technological foundations and the role of digital avatars. Following this, we provide a critical assessment of the operation of criminal law in the metaverse, which leads to the main thesis of this work: the need to develop a new multifactorial model of jurisdiction. This model, intended to rethink the concept of locus delicti in the metaverse, systematically defines jurisdiction based on a multi-pronged analysis of the offender's digital identity, the location of digital assets, platform management protocols, and the actual damage or physical connection caused by the virtual action.

1. Criminalization of the metaverse

Although some of the examples below are of a civil law nature, they can be used to outline landmarks useful for rethinking the concept of an incident in criminal law.

One of the most notable conflicts of legal interests arises in connection with the illegal use of intellectual property in the metaverse. A clear example of this is

2 Metaverse Market. Report ID: 101905. (2025). Market.us Scoop. https://clck.ru/3QGxSF

3 Ibid.

4 Ibid.

5 Duarte, F. (2025, June 5). Number of Metaverse Users in 2025. Exploding Topics. https://clck.ru/3QGxcm

6 Ibid.

the civil dispute between Roblox Corporation (further – Roblox), which develops and operates a virtual online entertainment platform, and WowWee Group Limited (further – WowWee), a leading developer, manufacturer, seller and distributor of innovative high-tech consumer robots, entertainment products and other gaming devices. Roblox, registered in California (USA), claimed that WowWee, registered in Hong Kong, illegally reproduced (copied) the design of Roblox virtual avatars to create and sell a line of physical minifigures (dolls) under the name My Avastars[7]. Based on the evidence presented, it was determined that WowWee intentionally sought to position these dolls as "real" versions of Roblox avatars, i.e. to establish a link between their physical product and the Roblox ecosystem, thereby using virtual intellectual property for material benefits[8].

As for criminal prosecution for infringement of copyright and related rights, the case presents a multifaceted jurisdictional dilemma, since it is necessary to determine the location of the crime (locus delicti). This may be Hong Kong, where WowWee is physically located; California (USA), where Roblox is located; the location of the servers (cloud, disk), where the data of the Roblox online platform are stored; or a decentralized virtual space (metaverse), where the original copyrighted avatar is located.

A similar dispute is between Impulse Communications, Inc. (a corporation from Delaware with headquarters in Rhode Island, USA) and Uplift Games LLC, Treetop Games LLC, Lionfield Investments LTD – companies that manage games with virtual pets called Adopt Me[9].

Another similar case occurred in a dispute between Hermès International (Paris, France) and Hermès of Paris, Inc. (New York, USA) and Mason Rothschild (Los Angeles, California, USA). Mr. Rothschild, operating from California, created and commercialized a collection of digital assets called MetaBirkins in the form of non-exchangeable tokens (NFTs), which were digital copies of the famous Hermès Birkin bag and were promoted as luxury items in the metaverse[10].

In the case of criminal prosecution for trademark infringement, the same serious problem of establishing a specific crime scene will arise. When determining jurisdiction, the crime scene may be the location of Hermès International (Paris, France); Hermès of Paris, Inc. (New York, USA); Mason Rothschild (California, USA); or the location of a decentralized blockchain network where infringing NFTs were created and sold.

---

7 Roblox Corporation et al v. WowWee Group Limited et al, No. 3:2022cv04476-SI – Document 69 (N.D. Cal. 2024). https://clck.ru/3QGxeC

8 Ibid.

9 Impulse Communications, Inc. v. Uplift Games, LLC et al, No. 24-cv-166-JJM-LDA – Document 29 (D.R.I. 2024). https://clck.ru/3QGxjZ

10 Hermes International et al v. Rothschild, No. 1:2022cv00384 – Document 140 (S.D.N.Y. 2023). https://clck.ru/3QGxnH

According to the indictment, in another case, the accomplices entered into a criminal conspiracy which acted from 2018 to 2022 to defraud investors of a group of companies owned by one of the attackers[11]. They raised funds promising to develop virtual technologies, including their own cryptocurrency, which was to be used in the metaverse they were creating[12]. They also promised knowingly unattainable high incomes and spread false claims that well-known entrepreneurs and wealthy buyers were involved in the acquisition[13]. Instead, they misappropriated funds for personal gain, including using the money to purchase personal real estate[14]. This case shows that if the entire scheme had been implemented in a fully decentralized metaverse without using traditional infrastructure, there would have been problems defining jurisdiction.

Finally, the most striking manifestation of the problem under consideration is probably the UK police investigation of crimes against sexual integrity committed in immersive virtual reality. As a result of the indecent acts, the victim allegedly suffered psychological and emotional trauma, which, despite the lack of physical contact, is an obvious sign of the objective element of crime[15]. An urgent question arises: where is the crime scene located if it was committed exclusively using avatars in virtual space? The crime scene can be determined by the physical coordinates of the victim or the perpetrator, or by the virtual environment (meta-territory) in which the crime was committed.

All these examples require a new legal approach to determining the crime scene, recognizing the metaverse as a full-fledged new space for crimes. This in turn, requires new principles for determining the operation of criminal law in space.

2. Principles of the operation of criminal law in space

2.1. Territorial principle

The main principle determining the operation of criminal law in space is the principle of territoriality. According to it, the state has exclusive jurisdiction to prosecute and punish crimes committed on its territory (Payer, 2023). A crime is considered committed on the territory of the Russian Federation if any of its constituent features, including the beginning, continuation or completion, took place within its state border (the doctrine

11 United States District Court District of Nebraska. (2025, June 4). 22-3077 – USA v. Chandran et al. [Government]. Administrative Office of the United States Courts. https://clck.ru/3QGxrp

12 Ibid.

13 Ibid.

14 Ibid.

15 Camber, R. (2024, January 1). British police probe VIRTUAL rape in metaverse: young girl's digital persona 'is sexually attacked by gang of adult men in immersive video game' – sparking first investigation of its kind and questions about extent current laws apply in online world. Daily Mail Online. https://clck.ru/3QGxwo

of subjective territoriality, the doctrine of objective territoriality, and the doctrine of effect (consequences) (Ryngaert, 2023).

The territory of the Russian state, defined by the Russian Constitution, includes land territory, water territory, subsoil and airspace (Part 1 of Article 67 of the Russian Constitution). The land territory covers the mainland and islands within the state border. The water territory comprises internal waters such as rivers and lakes, and a territorial sea – a strip of marine water area 12 nautical miles wide adjacent to land or inland waters (Part 1 of art. 2 of the Federal Law "On internal sea waters, territorial sea and contiguous zone of the Russian Federation")[16]. The subsoil is a part of the Earth crust below the Earth surface (the soil layer, and in its absence – below the Earth surface and the bottom of reservoirs and watercourses, extending to depths accessible for geological study and development) (preamble of the Federal Law "On subsoil")[17]. The airspace is an area above land and water with an assumed upper limit 100–110 km (conditional boundary between the Earth atmosphere and space (Karman line) (Pogorzelska, 2024).

The state border defining the sovereign territory of the Russian Federation is a vertical plane running along these physical borders. Outside of these defined zones, the territorial principle applies to certain crimes committed on the Russian continental shelf and in its exclusive economic zone. Both of these zones are marine areas outside the territorial sea, where the Russian Federation exercises special sovereign rights, in particular with regard to natural resources.

According to the territorial principle, Russian criminal law applies to crimes committed on civil ships and aircraft registered in the Russian Federation when they are in international waters or airspace, as well as on Russian military ships and aircraft, regardless of their location (Part 3 of Article 11 of the Russian Criminal Code)[18].

2.2. Exterritorial operation of criminal law

It is customary to distinguish cases in which a state's jurisdiction is assumed to be exercised beyond its national borders, known as extraterritorial jurisdiction. In this regard, the following principles are distinguished: active citizenship, passive citizenship, protective and universal jurisdiction.

The principle of active citizenship (personal, national) reflects the right of the state to exercise criminal jurisdiction over the deeds of its citizens who have committed

[16] On internal sea waters, territorial sea and contiguous zone of the Russian Federation. No. 155-FZ of July 31, 1998 (with amendments and additions, Federal Law of July 31, 2025 No. 304-FZ). Garant. https://clck.ru/3QGyAr

[17] On subsoil. No. 2395-I of February 21, 1992 (with amendments and additions, Federal Law of July 31, 2025 No. 353-FZ). KonsultantPlyus. https://clck.ru/3QGyCQ

[18] Criminal Code of the Russian Federation of June 13, 1996. No. 63-FZ. KonsultantPlyus. https://clck.ru/3QGyDx

criminally punishable deeds outside its territory, regardless of their geographical location (Esakov, 2015).

On the other hand, although it is the subject of scientific debate, the principle of passive citizenship (passive personal citizenship) implies exercising extraterritorial criminal jurisdiction by the state in relation to crimes where the victim is its citizen (Esakov, 2015). In this case, the crime is committed by foreign nationals (or stateless persons) outside the state border.

If a crime committed outside the state territory by a foreign citizen (or a stateless person) encroaches on the interests of that state, then the law of that state applies in accordance with the principle of protection (Esakov, 2015).

The principle of universality allows for the application of state law in the criminal prosecution of foreign citizens and stateless persons who have committed crimes against the peace and security of humankind. The application of this principle is justified due to considerations of international public policy (Esakov, 2015).

3. Phenomenon the metaverse: notion and ontological properties

The concept of the metaverse, which was once limited to the realm of science fiction, is now turning into a new reality, which in the future will give a new expression to human interaction in the digital dimension. In 1992, Neal Stephenson described the metaverse in his novel “Snow Crash” as a virtual reality that would replace the Internet (Ioannıdıs & Kontıs, 2023). Since then, the idea of the metaverse has improved significantly with the development of virtual reality (VR), augmented reality (AR), haptics, and artificial intelligence technologies.

The metaverse is a set of interconnected digital spaces and phenomena that combine a virtually enhanced physical reality and a physically stable virtual reality. Thus, there is a qualitative transition from the current stage of the Internet development to an immersive three-dimensional online environment. The network space proposed within the metaverse concept allows users to interact with each other and with the computer environment in real time, usually using digital avatars (Han et al., 2023). Its transformative potential extends to virtually all areas of human activity, including healthcare, education, work, social interaction, commerce, and entertainment.

Immersiveness

A characteristic feature of the metaverse is its ability to immerse users in three-dimensional space. This immersion is achieved through advanced augmented reality (XR) devices, which include virtual reality (VR) headsets, augmented reality (AR) devices, and mixed reality (MR) technology. These tools use stereoscopic images and spatial sound to create the illusion of depth and space, allowing users to feel “real” (telepresence) in a place other than their physical location (Bhowmik, 2024). The degree of sensory

immersion plays a crucial role in arousing emotions and influencing user behavior. Such a deep level of engagement means that virtual experiences can have a significant psychological impact, further blurring the line between the virtual and real worlds.

Synchronicity of interaction

The metaverse provides real-time interaction between users and the virtual environment (Hosseini et al., 2024). This kind of instantaneity is crucial for creating a dynamic and operational experience, allowing for synchronous social interaction, joint work, and flexible gameplay. The sense of "presence" is greatly enhanced by the instant adaptation of the user's vision and sensory feedback in response to their movements and actions (Hosseini et al., 2024). This reality means that actions and their consequences in the metaverse can be instantaneous.

Stability (constancy)

The next feature of the metaverse is its constancy, which ensures the continuous existence of the virtual world and all the changes taking place in it, even when users are not connected to the system (Richter & Richter, 2023). This means that users' avatars, digital twins (virtual representations of objects), and the state of the metaverse spaces remain unchanged over time, ensuring stability and integrity. Unlike traditional online games, where sessions end and progress can be reset or limited to specific episodes, a truly permanent metaverse implies a stable digital environment that evolves based on user actions and remains unchanged until users change it. Although modern platforms demonstrate a certain degree of local persistence, the general criterion of stable, universal persistence, as it is represented for the metaverse, remains an important area for technological progress and research.

Interoperability

Another feature of the metaverse is functional compatibility (interoperability), which is the ability to seamlessly move virtual digital objects, avatars, and data between different virtual worlds and platforms throughout the metaverse (Richter & Richter, 2023). It is this property that ensures the unity and interconnectedness of the digital universe. It significantly differs from the current mode, when virtual worlds are largely incompatible with each other and often remain "closed". It is generally recognized that to ensure genuine interoperability we need compatible technologies, equipment, protocols and standards that ensure the smooth exchange of information and simultaneous response of different systems.

Decentralization

The main feature of the metaverse is its decentralization, which implies the distribution of control and rights among network participants (McStay, 2023), rather than their concentration in the hands of a single central authority (provider). In fact, this is an integral principle of managing the metaverse, influencing decision-making, setting rules, and maintaining the overall structure of the virtual environment. The main instrument of decentralization is blockchain technology, which provides transparency and autonomy

by recording transactions and alterations in a publicly accessible and immutable registry (Panda, 2023). Such distributed control is aimed at empowering users by giving them more rights to their digital assets (such as virtual real estate, gaming items, and virtual currency) and direct participation in managerial decision-making, which reduces vulnerability to arbitrary actions by a central authority. Decentralization also helps to overcome censorship, since no organization is able to prescribe content or restrict access, and this promotes freedom of expression and creativity.

4. Technological basis of the metaverse

The metaverse functioning is based on the synergetic integration of various advanced technologies, forming a multi-level ecosystem that supports its immersive, constant and interactive characteristics.

Extended reality (XR) is an umbrella term that encompasses virtual reality (VR), augmented reality (AR), and mixed reality (MR). It is a range of immersive technologies used to access and interact with (in) the metaverse (Özkan & Özkan, 2024).

Virtual reality (VR) immerses users in a fully computer-generated, artificial three-dimensional environment. This is usually achieved using virtual reality headsets equipped with stereoscopic screens and spatial sound, creating a strong sense of presence (Bhowmik, 2024). Motion sensors track the user's movements, correcting the virtual view in real time, while tactile feedback devices can create a sense of touch, allowing users to manipulate virtual objects (Bhowmik, 2024).

Augmented reality (AR) superimposes digital data (elements, objects) on the physical world, improving the user's perception of reality (Bhowmik, 2024). Unlike VR, AR combines physical and digital elements, creating a holistic interface that integrates virtual content into the user's real-world environment, often using devices such as smartphones or transparent VR headset modules. With AR applications, users can interact with the displayed data as if they were real, access maps, or create shared AR experiences (Syed et al., 2022).

Mixed reality (MR) combines elements of VR and AR, allowing digital and real objects to coexist and interact in real time (Rokhsaritalemi et al., 2020). This technology is a more advanced form of mixing physical and virtual reality.

5. Digital avatars (digital twins)

In the metaverse, users employ virtual avatars as their digital representations through which they express themselves, communicate, and otherwise interact with others in virtual space (Kim et al., 2025). These avatars can be highly customizable, allowing users to express themselves in unique ways or even recreate characters from popular culture. The ability to create and embody digital identities goes beyond simple profile photos, representing personality, style, and even social status in the metaverse.

At the same time, the very concept of a digital personality in the metaverse remains complex and multifaceted, fundamentally different from a personality in the real world. In the digital space, one person can have several different and even pseudonymous identities, which complicates traditional concepts of identity and responsibility. The increasing convergence of real and virtual personalities means that harm caused to a user's avatar can have serious moral and legal consequences in the real world. Undoubtedly, with this understanding of digital identity, new legal issues arise regarding personal rights, fraud, and deception in a virtual environment.

6. Operation of criminal law in the metaverse

Traditional legal regulations basically focus on social relations in the physical world that develop between people located in a certain territory. By its nature, the metaverse transcends such physical boundaries, creating a global, interconnected digital space in which users from different countries can easily interact with each other. This fundamentally new circumstance means that actions performed in the virtual world can have consequences in the real world in several jurisdictions, as shown by the examples above. Consequently, it becomes much more difficult to determine which country's legislation is to be applied, as well as to establish the investigative and judicial jurisdiction of a criminal case.

Web 3, the next stage in the Internet development, is widely considered to pose new challenges in terms of accounting for geopolitical boundaries, but many online activities are still indirectly linked to the user's location through parameters such as language, time zone, domain names, IP addresses, and other metadata. Perhaps the most important and at the same time fraught with certain risks is the fact that immersion in a virtual world, especially one designed to mimic or (conditionally) replace the real world, does not imply a presumption of mandatory compliance with the laws of any particular country, with the possible exception of the rules of this platform (metaverse).

The limitations of the existing principles of determining jurisdiction and legal structures in terms of an appropriate response to the peculiar challenges of the metaverse indicate the need to develop new comprehensive legal approaches. A reactive approach, reduced to attempts to simply adapt existing legal norms to new digital realities, may not be sufficient and may lead to the constant appearance of gaps in legal regulation, especially in criminal law.

7. Multifactorial jurisdiction model: rethinking of the crime scene in the metaverse

Based on the above, we propose to revise the content of the "crime scene" concept in a decentralized metaverse and consider it not as a specific spatial point, but as a distributed system of individual components. In this system, each component (signs of a criminal deed both inside and outside the metaverse) is an independent link that defines jurisdiction.

It seems appropriate to determine jurisdiction based on a comprehensive analysis of all these components, not limited to a single, often arbitrary, location in physical space.

The main idea of the multifactorial jurisdiction model is to consider a crime as an event with several legally significant points of contact in digital and physical space, rather than as a deed committed in one specific geographical location. The model elements rely on the theoretical comprehension of the established legal principles of determining the criminal law operation in space and are designed to provide a structured and reliable basis for criminal prosecution.

The proposed model includes four key factors, each providing the court with a separate basis for determining criminal jurisdiction:

a) the subject (of a virtual deed);

b) digital assets;

c) platform protocols (code management);

d) harm (physical connection or final result).

7.1. Establishing jurisdiction in relation to the subjects of a virtual deed in the metaverse

Identification of a person who has committed crimes in the metaverse should be carried out based on information contained in a distributed registry (in other words, in blocks interconnected in a chain in a decentralized database (blockchain) (Komalavalli et al., 2020), or through a pseudonym associated with the offender's digital identity. In this case, an unchangeable and irreversible digital footprint of criminal activity is recorded.

The main distinguishing feature of a virtual action is its immutability. After being fixed, it is permanently recorded in a distributed ledger (blockchain), which makes it immutable and irreversible (Aakula et al., 2023). Each block contains cryptographic references to the previous block, a timestamp, and transaction data, which technically eliminates the possibility of changing information in a separate block without changing the entire chain (Aakula et al., 2023). This mechanism provides an exceptionally reliable and verifiable digital footprint of activity that can serve as reliable evidence.

The distributed nature of the action recording means that information is distributed across a network of interconnected nodes rather than being stored in a single centralized repository (Aakula et al., 2023). In this way, increased transparency, resistance to forgery, and global availability of records are achieved. Examples of virtual deeds are the transfer of digital assets, the use of malicious smart contracts (for example, when committing theft), or even virtual harassment. These actions, although they occur exclusively in a virtual environment, have tangible legal and economic consequences in the real world.

The main hypothesis is that the offender's address in the blockchain, by virtue of its verifiable, unchangeable and traceable activity, acquires a kind of legal equivalent of physical presence for the purposes of establishing personal jurisdiction.

This is a fundamental paradigm shift, establishing a new form of jurisdiction based on stable digital data and not limited to a temporary physical location. Such a conceptual shift facilitates the initiation of criminal prosecution based on the offender's verifiable and irreversible actions on the blockchain, even if their physical location remains unknown. This is consistent with the principles of due process by establishing a clear, digitally derived link between the suspect's unique digital identifier and the alleged offense.

The solved "blockchain paradox" is manifested by an internal contradiction: although transactions on the blockchain may seem anonymous due to the use of pseudonymous digital wallets, the main activity is traceable in principle. The offender's actual identity may remain unknown, but their digital activity in the distributed registry is constantly recorded and can be tracked using signature schemes and cryptographic hashes that reveal behavioral patterns (Trozze et al., 2022). The main task is to bridge the gap between monitored digital activity and a real person.

If a virtual action is an immutable and verifiable record, then the action per se becomes a "tangible", verifiable object in the digital space. This transforms a virtual action from a simple proof of human behavior into a digital object that can be the subject of research during a trial. We are talking not only about who committed the act, but also about what this act is and where it is recorded (in our case, in the blockchain). This extends the concept of substantive jurisdiction (jurisdiction in rem) beyond digital assets, extending it to digital actions per se. This means that the court can extend its jurisdiction over virtual actions as a separate legal fiction (digital "thing" or "events"), which will allow for investigations, injunctions (for example, blocking smart contract functions), or even "removing" a digital footprint, even before the offender is identified or physically detected. This is a significant extension of the in rem principles to the field of digital behavior, providing a powerful new tool for law enforcement in decentralized environments.

To implement the above, it may be necessary to develop and implement special regulations requiring centralized exchanges and other services to store information about their customers and provide it upon appropriate official request.

This includes collecting and verifying personal information, like full name, date of birth, residential address, and a standard ID. The introduction of such a standard at the international level would allow obliging exchanges around the world to store such data and provide it upon legitimate request, thereby establishing an important link between a blockchain address and a real person. This would significantly expand the capabilities of law enforcement agencies in overcoming the blockchain paradox by providing legitimate access to identification data.

However, it should be noted that the existence of decentralized exchanges (DEXs), which often do not collect this information, is a problem that requires a separate scientific study.

7.2. Digital assets as the basis for establishing jurisdiction in rem

Digital assets, including cryptocurrencies, non-fungible tokens (NFTs), and in-game (computer) items, are generally recognized as a separate type of property (or, more precisely, rights) that can be used in criminal activity as an object or means of crime. Their official classification as a new form of property allows them to be directly subject to the established principle of substantive jurisdiction. This principle makes it possible to exercise jurisdiction over disputed property located within the territorial jurisdiction, regardless of the physical location of its owner (Niesel, 2023). Such a legal classification is crucial because it allows the seizure of property and, if necessary, its confiscation, which are the object (means) of criminal activity, thereby guaranteeing the possibility of recourse to legal protection and the return of property in the digital sphere.

Although the blockchain per se serves as the main location of digital assets (and in fact the storage server), their practical digital location can be deduced from a number of circumstances. Jurisdiction can actually be established where a digital asset interacts with the physical world. A striking example is the situation when digital assets were acquired or disposed of using fiat currency through a local banking institution; this creates a clear and indisputable link to a specific physical territory.

Centralized platforms, such as exchanges, perform an essential function in this case, acting as entry (and exit) points between the metaverse and the real world. The jurisdiction of the court at their location extends to the activities of these exchanges, which allows seizing or freezing assets stored on the accounts of these platforms.

An alternative option for establishing jurisdiction is the location of the hosting provider, on whose server a certain segment of the decentralized network is located. This approach is based on the identification and use of the Internet physical infrastructure (cables, servers, data centers), which underlies even the most decentralized digital operations. In the legal analysis of intangible assets, a legal fiction is often created to link these assets to a specific location, taking into account factors such as the effectiveness of law enforcement and access to legal remedies (Wendehorst, 2023). In some cases, this may imply the physical location of a digital wallet if it can be reliably linked to a specific person.

The above approaches to asset location demonstrate the crucial, often overlooked relationship between centralized gateways and decentralized networks for enforcement purposes. Centralized exchanges by their nature provide a regulated “point of control” where a real personality and physical location can be linked to digital assets in accordance with the requirements of anti-money laundering and terrorist financing legislation (Schuler et al., 2024). However, purely decentralized assets or transactions, although more difficult to seize directly, still depend on the underlying physical infrastructure (nodes, servers, hosting providers) for their operation (Schuler et al., 2024; Bains et al., 2022).

All this indicates the need for dual regulation: for digital assets interacting with the traditional financial system or centralized service providers, the use of these centralized structures is of paramount importance for effective legally meaningful measures. For truly decentralized assets bypassing such gateways, the focus shifts to identifying and asserting jurisdiction over the physical infrastructure supporting the network. This highlights the fundamental contradiction between the decentralized ideal of the metaverse and the practical reality of law enforcement, implying that even the most "limitless" digital assets are ultimately tied to physical reality to one degree or another, whether through human interaction with centralized services or through the underlying computing infrastructure.

7.3. Platform protocols (code management) as the basis for establishing jurisdiction

In terms of establishing jurisdiction, the protocol refers to the underlying blockchain network or a set of rules (code) governing the virtual space in which the offense was committed. It provides a technical framework and automated rules embedded in the system. A decentralized autonomous organization (further – DAO), on the contrary, is a form of managing this virtual space, often built on the basis of a specific protocol or interacting with it (Qin et al., 2022). It functions as an organizational structure, usually managed by decentralized software, with voting and finances processed through the blockchain (Qin et al., 2022). An offense can be committed both by using a protocol (for example, the deployment of a malicious smart contract), and within the DAO (for example, by falsifying voting in its management system).

The principle of "code management" as the basis of jurisdiction is based on the following legal theory. A DAO, by its very nature, as a self-governed and self-regulated structure, can be involved in criminal activities such as laundering (legalization) of criminal proceeds (Benson et al., 2024) or fraud (Scharfman, 2024) (through its representatives or collective actions of token holders or third parties). This is analogous to traditional legal entities, such as commercial organizations or government agencies. Just as a commercial organization is a legal entity capable of bearing legal (administrative, civil) responsibility for its actions, a DAO, through code-based management and collective decision-making, can be recognized as a legal entity in certain jurisdictions. The "code rule" (Judge et al., 2025), which regulates operations and transactions on the blockchain, provides a form of responsibility on the chain.

Jurisdiction may be extended to individuals who have created, deployed, or actively control the protocol, provided that they are physically located within the jurisdiction of the relevant state. Thus, traditional personal jurisdiction is applied when there is a link to a person, which provides direct contact for law enforcement.

Formal legal structures transform a decentralized protocol or DAO from a "shadow" or ambiguous network into a legally recognized organization with a specific location and legal personality (Pesqueira, 2025). This is crucial in order to avoid ambiguous qualifications of the deed, which can lead to unlimited personal liability of individual token holders, thus deterring participation in the activities of the organization. Turning to foreign experience, one can note that some US states (for example, Wyoming[19], Vermont[20], Tennessee[21] and the Republic of the Marshall Islands[22]) have adopted laws recognizing DAOs as legal entities, usually in the form of a decentralized autonomous organization with limited liability (DAO LLC). Such legal recognition ensures predictability, limited liability of participants (similar to traditional LLCs) and the ability of DAOs to enter into civil law relations, i.e. conclude contracts, own property, and interact with traditional legal systems.

At the same time, the inherent global and decentralized nature of the DAOs means that they can affect social relations that arise in the territories of different jurisdictions.

Therefore, there is a contradiction between the ideal of decentralization and the need to ensure legal responsibility. Decentralization implies the distribution of control and stability to a central authority, while the proposed solution for jurisdiction over protocols and DAO is largely based on the creation of formal legal structures and legal status for DAO (as was done in a number of US states mentioned above). This is a direct conceptual contradiction. The essence of decentralization is to eliminate single points of control and authority, which naturally makes it difficult for traditional legal systems to identify a responsible party. The imposition of a legal "shell" or the requirement to register as an LLC, in fact, reintroduces a certain degree of centralization or identifiable legal personality. Being necessary to establish legal responsibility, this may be perceived as compromising the basic principles of decentralization, in addition restraining innovation in this field.

The main challenge is to achieve a pragmatic balance in which legal responsibility can be implemented without compromising the fundamental advantages of decentralization, such as freedom from censorship and promotion of innovative initiatives. This

---

19 WY Stat § 17-31-101 (2024). 2024 Wyoming Statutes, Title 17 – Corporations, Partnerships and Associations, Chapter 31 - Decentralized Autonomous Organization Supplement, Article 1 – Provisions, Section 17-31-101 – Short Title. https://clck.ru/3QGyrv

20 11 VT Stats § 4171. 2024 Vermont Statutes, Title 11 – Corporations, Partnerships and Associations, Chapter 25 – Limited Liability Companies, § 4171. Definitions. https://clck.ru/3QUdkt

21 TN Code § 48-250-101 (2024). 2024 Tennessee Code, Title 48 – Corporations and Associations (§ 48-1-101 – 48-250-115) Limited Liability Companies (§ 48-201-101 – 48-250-115), Chapter 250 – Blockchains (§§ 48-250-101 – 48-250-115), Section 48-250-101 – Chapter definitions. https://clck.ru/3QwuTB

22 52 MIRC Ch. 7 § 701. Republic of the Marshall Islands Code, Title 52 – Associations Law, Chapter 7 – Decentralized Autonomous Organization Act 2022. https://clck.ru/3QwuHz

presupposes a future legal environment in which hybrid legal structures will increasingly prevail, combining aspects of decentralized governance with traditional legal personality.

7.4. Harm (physical connection or ultimate result) as the basis for establishing jurisdiction

Harm (physical connection or ultimate result) is the only physically determined element in the multifactorial jurisdiction model. It acts as the most important link to the real world, which connects a virtual offense with its material, legally significant consequences for an individual or organization. This factor directly fits into and expands the existing legal doctrine of consequences, according to which jurisdiction can be established based on the negative consequences of a deed that occurred in a certain territory. Its main purpose is to ensure that the victim has access to justice in court at his place of residence, providing a clear and accessible way to recover damages, regardless of the virtual nature of the original deed.

The harm factor serves as an important starting point for establishing jurisdiction in cases where other factors (such as the perpetrator identity, the specific location of digital assets) may be ambiguous or inaccessible. It transforms the abstract nature of crimes in the metaverse into specific legal constructions that correspond to existing, established legal norms. In addition, this factor suggests that victims are not left without legal protection just because the crime was committed in a new digital environment, which means that the fundamental principle of access to justice will be respected. Apparently, this also means that in court proceedings involving crimes in the metaverse, it will be of paramount importance to prove a clear and direct causal relationship between virtual action and real damage.

In this study, we highlight only psychological harm, reputational damage, and material damage as examples of harm from metacrimes.

Psychological harm is an obvious and widespread type of harm that can be inflicted in a virtual environment. The experience of virtual realities, especially immersive ones created with the help of virtual and augmented reality (VR/AR) technologies, can cause genuine psychological and emotional reactions, making the harm experienced in virtual space as real and significant as the harm caused in the physical environment. A prime example is the UK police investigation into lewd acts committed in immersive virtual reality, during which, according to reports, the victim suffered “psychological and emotional trauma” despite the absence of physical contact[23].

[23] Camber, R. (2024). British police probe VIRTUAL rape in metaverse: young girl’s digital persona ’is sexually attacked by gang of adult men in immersive video game’– sparking first investigation of its kind and questions about extent current laws apply in online world. Daily Mail Online. https://clck.ru/3QGzVQ

Reputational damage caused in the metaverse (for example, dissemination of false brand information, unauthorized use of trademarks on virtual goods, or sale of counterfeit virtual items) can lead to significant and measurable damage to the reputation and financial standing of a company or individual in the real world. A clear illustration is the case Hermès v. Rothschild, when the creation and commercialization of MetaBirkins NFT was recognized as a violation and dilution of trademark rights, which caused reputational and financial damage to Hermès[24].

Material damage, in addition to direct financial damage, covers damage caused to the "digital twin" of a real object, which, in turn, leads to damage to the physical object per se. Digital twins are virtual representations of physical objects, processes, or systems that dynamically simulate and predict the behavior of their (real) physical prototypes (Segovia & Garcia-Alfaro, 2022). They are integrated with real-time data (Segovia & Garcia-Alfaro, 2022), which means that malicious actions or vulnerabilities exploited in the digital twin can directly manifest as damage or failure in the physical twin. In this context, the use of cyber-physical systems is a recognized risk.

The nature of these forms of harm – intangible, digitally mediated, or associated with complex interactions of digital twins – creates significant and unavoidable difficulties with proving. Documenting psychological harm from a virtual deed requires overcoming traditional skepticism about the virtual nature of harm, which is considered less real, which necessitates reliable psychological and medical methods of proving. Reputational damage, although it has tangible consequences, is often diffuse, difficult to quantify accurately, and can spread rapidly in the digital space. Material damage caused to digital twins requires highly specialized forensic computer analysis to establish an accurate cause-and-effect relationship between the digital attack and the physical consequences. In these cases, the case is not limited to "classical" physical evidence.

All this indicates a significant and growing demand for specialized forensic expertise (for example, digital psychologists, brand evaluators, forensic analysts of cyber-physical systems) and for the development of new legal standards for digital evidence. The rules of proving should be adapted to account for and evaluate new forms of evidence related to intangible and digital-mediated damage.

Conclusion

The development of virtual worlds, a metaverse with their inherent properties of decentralization, stability and immersiveness, makes it difficult to apply the traditional principles of determining the operation of criminal law in space. Well-established legal

[24] Hermes International et al v. Rothschild, No. 1:2022cv00384 – Document 140 (S.D.N.Y. 2023). https://clck.ru/3QGzYA

approaches, conditioned by the physical borders (territory) of the state and the interaction of persons in objective reality, turn out to be untenable in relation to crimes committed in virtual spaces that do not have defined boundaries. The cases cited in this paper, ranging from violations of intellectual property rights to property crimes and crimes against sexual integrity, confirm the existence of a serious gap in modern criminal law regarding the definition of the crime scene in the metaverse.

In order to overcome this deepening jurisdictional gap, this article proposes a multifactorial model of jurisdiction in which the crime scene is considered not as a specific point in space, but as a distributed system consisting of individual components. This paradigm shift, based on an analysis of the offender's digital identity, the nature and location of digital assets, management protocols embedded in the platform code, and the material damage caused, allows for a comprehensive framework for determining criminal jurisdiction.

In particular, the model substantiates that the immutable and verifiable nature of blockchain transactions can serve as the legal equivalent of a physical presence to establish personal jurisdiction. In addition, the classification of digital assets as an independent form of property allows direct application of in rem jurisdiction, while the principle of "code management" helps to establish jurisdiction over organizations or individuals responsible for the protocol development and control. At the same time, the harm factor ensures victims' access to justice, linking virtual offenses with their material consequences in the physical world.

For all its theoretical persuasiveness and expediency, the proposed model is not devoid of internal limitations that force one to assess it critically. The establishment of jurisdiction based on the offender's digital identity, although theoretically justified, largely depends on overcoming the "blockchain paradox" – the internal contradiction between the anonymity of pseudonymous digital wallets and the traceability of basic activity. The effectiveness of this approach depends on the development and implementation (at the global level) of strict rules for centralized exchanges and the future creation of mechanisms to identify the persons behind decentralized identification data. The problem posed by completely decentralized exchanges (DEXs), which often circumvent such data collection measures, remains a major obstacle requiring further scientific research and legal regulation.

Similarly, although the classification of digital assets as property simplifies the application of in rem jurisdiction, practical enforcement mechanisms for assets located exclusively in decentralized networks, without interaction with centralized gateways, remain insufficiently developed. Dependence on the identification of the Internet physical infrastructure (for example, hosting providers) to establish jurisdiction over purely decentralized assets, although necessary, is a conceptual contradiction with the very essence of decentralization.

The principle of "code management" as a jurisdictional link also presents a semantic dilemma. The proposal to provide formal legal structures and status to decentralized autonomous organizations, while extremely important for ensuring the unavoidable responsibility, inherently reintroduces a certain degree of centralization, which contradicts the fundamental principles of decentralization. A pragmatic balance between ensuring legal responsibility and preserving the main advantages of decentralization, such as the absence of censorship and the innovation promotion, requires constant discussion and the potential development of hybrid legal structures.

Finally, although the harm factor provides an important physical connection, the intangible and digitally mediated nature of harm such as mental suffering, reputational damage, and damage caused to digital twins is fraught with certain difficulties in proving. To overcome traditional skepticism about the virtual nature of harm, we need to develop new research methodologies, as well as to adapt the rules of evidence to account for and evaluate these new forms of digital evidence.

Therefore, future research should focus on a number of important areas. First, it is advisable to conduct comparative legal studies to clarify how different jurisdictions are currently dealing with these issues and to identify best practices for cross-border cooperation in investigations of crimes related to the metaverse. Second, it is extremely important to develop standardized international protocols on data exchange and mutual legal assistance in the search and collection of evidence based on blockchain technology. Third, interdisciplinary research involving legal scholars and computer scientists is crucial for clarifying the technical and conceptual understanding of digital identity, ownership of digital assets, and the nature of damage in virtual environments. Finally, we believe that legislative initiatives should go beyond reactive adaptation but proactively create a comprehensive legal framework that should be inherently scalable and sustainable under the rapid technological changes characteristic of the metaverse. Only through such concerted and collaborative efforts can the international community hope to create a reliable and fair system of justice in the emerging digital environment of the metaverse.

References

Aakula, A., Sandhu, K., Srinivasan Venkataramanan, V., Alluri, R. R., & Saini, V. (2023). Forging Unbreakable Identities: The Biometric-Blockchain Nexus. *Nanotechnology Perceptions*, *19*, 644–652. https://doi.org/10.62441/nano-ntp.v19i3.5078

Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022). Regulating the crypto ecosystem: The case of unbacked crypto assets. *International Monetary Fund*.

Benson, V., Turksen, U., & Adamyk, B. (2024). Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance*, *32*(1), 80–97. https://doi.org/10.1108/JFRC-04-2023-0065

Bhowmik, A. K. (2024). Virtual and augmented reality: Human sensory-perceptual requirements and trends for immersive spatial computing experiences. *Journal of the Society for Information Display*, *32*(8), 605–646. https://doi.org/10.1002/jsid.2001

Brey, P. (2025). Will There Be a Metaverse? In The Metaverse: A Critical Assessment. *SpringerBriefs in Ethics* (pp. 33–57). Springer, Cham. https://doi.org/10.1007/978-3-031-93471-1_3

Chimni, B. S. (2022). The international law of jurisdiction: A TWAIL perspective. *Leiden Journal of International Law*, *35*(1), 29–54. https://doi.org/10.1017/S0922156521000534

Esakov, G. A. (2015). Extraterritorial criminal jurisdiction: contemporary global trends. *Statute*, *8*, 82–89. (In Russ.).

Han, E., Miller, M. R., DeVeaux, C., Jun, H., Nowak, K. L., Hancock, J. T., Ram, N., & Bailenson, J. N. (2023). People, places, and time: a large-scale, longitudinal study of transformed avatars and environmental context in group interaction in the metaverse. *Journal of Computer-Mediated Communication*, *28*(2), zmac031. https://doi.org/10.1093/jcmc/zmac031

Hosseini, S., Abbasi, A., Magalhaes, L. G., Fonseca, J. C., da Costa, N. M., Moreira, A. H., & Borges, J. (2024). Immersive interaction in digital factory: Metaverse in manufacturing. *Procedia Computer Science*, *232*, 2310–2320. https://doi.org/10.1016/j.procs.2024.02.050

Ioannıdıs, S., & Kontıs, A. P. (2023). The 4 Epochs of the Metaverse. *Journal of Metaverse*, *3*(2), 152–165. https://doi.org/10.57019/jmv.1294970

Judge, B., Nitzberg, M., & Russell, S. (2025). When code isn't law: rethinking regulation for artificial intelligence. *Policy and Society*, *44*(1), 85–97. https://doi.org/10.1093/polsoc/puae020

Kim, H. S., Kim, S., & Lee, E. J. (2025). The mirror of the metaverse: an exploration of reciprocal effects between self-views and avatar-based self-presentation. *Human Communication Research*, *51*(3), 142–152. https://doi.org/10.1093/hcr/hqaf005

Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In *Handbook of research on blockchain technology* (pp. 349–371). Academic Press.

McStay, A. (2023). The metaverse: Surveillant physics, virtual realist governance, and the missing commons. *Philosophy & Technology*, *36*(1), 13. https://doi.org/10.1007/s13347-023-00613-y

Niesel, Z. (2023). Crypto Contacts: Jurisdiction and the Blockchain. *Tulane Law Review*, *98*, 917.

Özkan, A., & Özkan, H. (2024). Meta: XR-AR-MR and mirror world technologies business impact of metaverse. *Journal of Metaverse*, *4*(1), 21–32. https://doi.org/10.57019/jmv.1344489

Panda, S. K. (2023). Revolution of the metaverse and blockchain technology. In *Metaverse and immersive technologies: An introduction to industrial, business and social applications* (pp. 97–125). https://doi.org/10.1002/9781394177165.ch4

Payer, A. (2023). The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries. *International Criminal Law Review*, *23*(2), 175–238. https://doi.org/10.1163/15718123-bja10151

Pesqueira, A. (2025). The Impact and Potential. In A. Pesqueira, & A. de Bem Machado (Eds.), *Navigating Privacy, Innovation, and Patient Empowerment Through Ethical Healthcare Technology* (pp. 217–254). IGI Global. https://doi.org/10.4018/979-8-3693-7630-0

Pogorzelska, K. (2024). Does Using Satellite Data for Sustainable Development Justify Unsustainable Use of Outer Space? In *Regulation of Outer Space* (pp. 7–25). Routledge. https://doi.org/10.4324/9781003512677

Qin, R., Ding, W., Li, J., Guan, S., Wang, G., Ren, Y., & Qu, Z. (2022). Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *53*(4), 2073–2082. https://doi.org/10.1109/TSMC.2022.3228530

Richter, S., & Richter, A. (2023). What is novel about the Metaverse? *International Journal of Information Management*, *73*, 102684. https://doi.org/10.1016/j.ijinfomgt.2023.102684

Rokhsaritalemi, S., Sadeghi-Niaraki, A., & Choi, S. M. (2020). A review on mixed reality: Current trends, challenges and prospects. *Applied Sciences*, *10*(2), 636. https://doi.org/10.3390/app10020636

Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, *24*(3), 537–550. https://doi.org/10.1017/glj.2023.24

Scharfman, J. (2024). Decentralized autonomous organization (dao) fraud, hacks, and controversies. In *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks* (pp. 65–106). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-60836-0_3

Schuler, K., Cloots, A. S., & Schär, F. (2024). On DeFi and on-chain CeFi: how (not) to regulate decentralized finance. *Journal of Financial Regulation*, *10*(2), 213–242. https://doi.org/10.1093/jfr/fjad014

Segovia, M., & Garcia-Alfaro, J. (2022). Design, modeling and implementation of digital twins. *Sensors*, *22*(14), 5396. https://doi.org/10.3390/s22145396

Syed, T. A., Siddiqui, M. S., Abdullah, H. B., Jan, S., Namoun, A., Alzahrani, A., Nadeem, A., & Alkhodre, A. B. (2022). In-depth review of augmented reality: Tracking technologies, development tools, AR displays, collaborative AR, and security concerns. *Sensors*, *23*(1), 146. https://doi.org/10.3390/s23010146

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1), 1. https://doi.org/10.1186/s40163-021-00163-8

Wei, W. (2023). Using actor–network theory to revisit the digitalized tool in social design. *The Design Journal*, *27*(1), 49–67. https://doi.org/10.1080/14606925.2023.2279836

Wendehorst, C. (2023). Proprietary rights in digital assets and the conflict of laws. In *Blockchain and Private International Law* (pp. 101–127). Brill Nijhoff. https://doi.org/10.1163/9789004514850_007

Author information

Murad M. Madzhumaev – Cand. Sci. (Law), Leading researcher, Senior Lecturer, Department of Criminal Law, Criminal Procedure and Criminology, Institute of Law, Peoples' Friendship University of Russia named after Patrice Lumumba
Address: 6 Miklukho-Maklaya Str., 117198 Moscow, Russia
E-mail: murad.mad@outlook.com
ORCID ID: https://orcid.org/0000-0003-3332-2850
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58624042900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ABB-9737-2021
Google Scholar ID: https://scholar.google.com/citations?user=qpGC84MAAAAJ
RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=1212027

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research was made under the grant of the Russian Scientific Fund No. 25-28-01478. https://rscf.ru/project/25-28-01478/

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – August 21, 2025
Date of approval – September 4, 2025
Date of acceptance – December 20, 2025
Date of online placement – December 25, 2025

Научная статья
УДК 34:004:343.213.3:343.232:343.235.4
EDN: https://elibrary.ru/rowsaq
DOI: https://doi.org/10.21202/jdtl.2025.23

Многофакторная модель юрисдикции: переосмысление места преступления в децентрализованной метавселенной

Мурад Мамедович Маджумаев

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Ключевые слова

аватар,
виртуальная реальность,
дополненная реальность,
место преступления,
метавселенная,
право,
преступление,
уголовное право,
цифровые технологии,
юрисдикция

Аннотация

Цель: провести критический анализ возможности распространения существующих принципов действия уголовного закона в пространстве на деяния, совершенные в децентрализованных виртуальных мирах метавселенной, и разработать предложения, включающие обновление подхода к установлению юрисдикции в отношении таких виртуальных преступлений.

Методы: методологическую основу исследования составляет совокупность общенаучных методов и подходов научного познания – диалектический, формально-логический (анализ и синтез, индукция и дедукция), системный, а также частно-научные методы – формально-правовой, правовое моделирование, толкование. Исследование опирается на анализ судебной практики, зарубежного законодательства, технических особенностей блокчейн-технологий и децентрализованных автономных организаций, что позволяет выявить пробелы в правовом регулировании и предложить концептуально новые решения для определения места совершения преступления в виртуальной среде.

Результаты: выявлена ограниченность реализации существующих общепринятых принципов определения юрисдикции в отношении виртуальных преступлений, которые не имеют физических координат. Предлагаемая многофакторная модель юрисдикции переопределяет «место преступления» с учетом таких факторов, как цифровая идентичность правонарушителя, характер и местонахождение цифровых активов, протоколы управления платформой и причиненный реальный ущерб. Предполагается, что неизменяемый и верифицируемый характер операций в блокчейне может служить своеобразным юридическим эквивалентом физического присутствия для установления персональной юрисдикции, позволяя инициировать уголовное преследование даже в тех случаях, когда фактическое местонахождение правонарушителя остается неизвестным.

Научная новизна: в работе изложен подход, предполагающий фундаментальное преобразование реактивных, адаптивных принципов правового регулирования в проактивную, комплексную основу, предназначенную специально для уникальных вызовов метавселенной. Выдвинута меняющая парадигму гипотеза, которая заключается в том, что постоянный (устойчивый) цифровой след правонарушителя в виртуальных пространствах может служить основой для осуществления юрисдикции. В модели системно увязано представление о вреде как важнейшем звене между виртуальными правонарушениями и их последствиями в реальном мире.

Практическая значимость: обусловлена отсутствием в настоящее время возможности применения к отношениям в метавселенной правовых норм и правил, учитывающих их специфику. Основные положения и выводы исследования могут быть использованы для совершенствования механизмов правового регулирования метавселенной, формирования международных протоколов об обмене данными и взаимной правовой помощи в вопросах поиска и сбора доказательств, основанных на технологии блокчейн, а также для разработки законодательных инициатив, направленных на создание комплексных правовых механизмов, масштабируемых и устойчивых к быстрым технологическим изменениям, характерным для цифровой среды.

Для цитирования

Маджумаев, М. М. (2025). Многофакторная модель юрисдикции: переосмысление места преступления в децентрализованной метавселенной. *Journal of Digital Technologies and Law*, *3*(4), 570–597. https://doi.org/10.21202/jdtl.2025.23

Список литературы

Есаков, Г. А. (2015). Экстратерриториальное действие уголовного закона: современные мировые тенденции. *Закон*, *8*, 82–89. https://elibrary.ru/uhlbaf

Aakula, A., Sandhu, K., Srinivasan Venkataramanan, V., Alluri, R. R., & Saini, V. (2023). Forging Unbreakable Identities: The Biometric-Blockchain Nexus. *Nanotechnology Perceptions*, *19*, 644–652. https://doi.org/10.62441/nano-ntp.v19i3.5078

Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022). Regulating the crypto ecosystem: The case of unbacked crypto assets. *International Monetary Fund*.

Benson, V., Turksen, U., & Adamyk, B. (2024). Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance*, *32*(1), 80–97. EDN: https://elibrary.ru/fgebbr. DOI: https://doi.org/10.1108/JFRC-04-2023-0065

Bhowmik, A. K. (2024). Virtual and augmented reality: Human sensory-perceptual requirements and trends for immersive spatial computing experiences. *Journal of the Society for Information Display*, *32*(8), 605–646. EDN: https://elibrary.ru/bxivih. DOI: https://doi.org/10.1002/jsid.2001

Brey, P. (2025). Will There Be a Metaverse? In *The Metaverse: A Critical Assessment. SpringerBriefs in Ethics* (pp. 33–57). Springer, Cham. https://doi.org/10.1007/978-3-031-93471-1_3

Chimni, B. S. (2022). The international law of jurisdiction: A TWAIL perspective. *Leiden Journal of International Law*, *35*(1), 29–54. EDN: https://elibrary.ru/gqkwgf. DOI: https://doi.org/10.1017/S0922156521000534

Han, E., Miller, M. R., DeVeaux, C., Jun, H., Nowak, K. L., Hancock, J. T., Ram, N., & Bailenson, J. N. (2023). People, places, and time: a large-scale, longitudinal study of transformed avatars and environmental context in group interaction in the metaverse. *Journal of Computer-Mediated Communication*, *28*(2), zmac031. EDN: https://elibrary.ru/qlwgxi. DOI: https://doi.org/10.1093/jcmc/zmac031

Hosseini, S., Abbasi, A., Magalhaes, L. G., Fonseca, J. C., da Costa, N. M., Moreira, A. H., & Borges, J. (2024). Immersive interaction in digital factory: Metaverse in manufacturing. *Procedia Computer Science*, *232*, 2310–2320. EDN: https://elibrary.ru/skunaz. DOI: https://doi.org/10.1016/j.procs.2024.02.050

Ioannıdıs, S., & Kontıs, A. P. (2023). The 4 Epochs of the Metaverse. *Journal of Metaverse*, *3*(2), 152–165. EDN: https://elibrary.ru/mwvqcn. DOI: https://doi.org/10.57019/jmv.1294970

Judge, B., Nitzberg, M., & Russell, S. (2025). When code isn't law: rethinking regulation for artificial intelligence. *Policy and Society*, *44*(1), 85–97. https://doi.org/10.1093/polsoc/puae020

Kim, H. S., Kim, S., & Lee, E. J. (2025). The mirror of the metaverse: an exploration of reciprocal effects between self-views and avatar-based self-presentation. *Human Communication Research*, *51*(3), 142–152. https://doi.org/10.1093/hcr/hqaf005

Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In *Handbook of research on blockchain technology* (pp. 349–371). Academic Press. https://doi.org/10.1016/B978-0-12-819816-2.00014-9

McStay, A. (2023). The metaverse: Surveillant physics, virtual realist governance, and the missing commons. *Philosophy & Technology*, *36*(1), 13. EDN: https://elibrary.ru/rgzoum. DOI: https://doi.org/10.1007/s13347-023-00613-y

Niesel, Z. (2023). Crypto Contacts: Jurisdiction and the Blockchain. *Tulane Law Review*, *98*, 917.

Özkan, A., & Özkan, H. (2024). Meta: XR-AR-MR and mirror world technologies business impact of metaverse. *Journal of Metaverse*, *4*(1), 21–32. https://doi.org/10.57019/jmv.1344489

Panda, S. K. (2023). Revolution of the metaverse and blockchain technology. In *Metaverse and immersive technologies: An introduction to industrial, business and social applications* (pp. 97–125). https://doi.org/10.1002/9781394177165.ch4

Payer, A. (2023). The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries. *International Criminal Law Review*, *23*(2), 175–238. EDN: https://elibrary.ru/ipnrgk. DOI: https://doi.org/10.1163/15718123-bja10151

Pesqueira, A. (2025). The Impact and Potential. In A. Pesqueira, & A. de Bem Machado (Eds.), *Navigating Privacy, Innovation, and Patient Empowerment Through Ethical Healthcare Technology* (pp. 217–254). IGI Global. https://doi.org/10.4018/979-8-3693-7630-

Pogorzelska, K. (2024). Does Using Satellite Data for Sustainable Development Justify Unsustainable Use of Outer Space? In *Regulation of Outer Space* (pp. 7–25). Routledge. https://doi.org/10.4324/9781003512677

Qin, R., Ding, W., Li, J., Guan, S., Wang, G., Ren, Y., & Qu, Z. (2022). Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *53*(4), 2073–2082. https://doi.org/10.1109/TSMC.2022.3228530

Richter, S., & Richter, A. (2023). What is novel about the Metaverse? *International Journal of Information Management*, *73*, 102684. EDN: https://elibrary.ru/sxufzu. DOI: https://doi.org/10.1016/j.ijinfomgt.2023.102684

Rokhsaritalemi, S., Sadeghi-Niaraki, A., & Choi, S. M. (2020). A review on mixed reality: Current trends, challenges and prospects. *Applied Sciences*, *10*(2), 636. EDN: https://elibrary.ru/hgwqbi. DOI: https://doi.org/10.3390/app10020636

Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, *24*(3), 537–550. EDN: https://elibrary.ru/dbquas. DOI: https://doi.org/10.1017/glj.2023.24

Scharfman, J. (2024). Decentralized autonomous organization (dao) fraud, hacks, and controversies. In *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks* (pp. 65–106). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-60836-0_3

Schuler, K., Cloots, A. S., & Schär, F. (2024). On DeFi and on-chain CeFi: how (not) to regulate decentralized finance. *Journal of Financial Regulation*, *10*(2), 213–242. EDN: https://elibrary.ru/kjghty. DOI: https://doi.org/10.1093/jfr/fjad014

Segovia, M., & Garcia-Alfaro, J. (2022). Design, modeling and implementation of digital twins. *Sensors*, *22*(14), 5396. EDN: https://elibrary.ru/whsffs. DOI: https://doi.org/10.3390/s22145396

Syed, T. A., Siddiqui, M. S., Abdullah, H. B., Jan, S., Namoun, A., Alzahrani, A., Nadeem, A., & Alkhodre, A. B. (2022). In-depth review of augmented reality: Tracking technologies, development tools, AR displays, collaborative AR, and security concerns. *Sensors*, *23*(1), 146. EDN: https://elibrary.ru/rxwauu. DOI: https://doi.org/10.3390/s23010146

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1), 1. EDN: https://elibrary.ru/kwtfwh. DOI: https://doi.org/10.1186/s40163-021-00163-8

Wei, W. (2023). Using actor–network theory to revisit the digitalized tool in social design. *The Design Journal*, *27*(1), 49–67. https://doi.org/10.1080/14606925.2023.2279836

Wendehorst, C. (2023). Proprietary rights in digital assets and the conflict of laws. In *Blockchain and Private International Law* (pp. 101–127). Brill Nijhoff. https://doi.org/10.1163/9789004514850_007

Сведения об авторе

Маджумаев Мурад Мамедович – кандидат юридических наук, ведущий научный сотрудник, старший преподаватель кафедры уголовного права, уголовного процесса и криминалистики Юридического института, Российский университет дружбы народов имени Патриса Лумумбы
Адрес: 117198, Россия, г. Москва, ул. Миклухо-Маклая, д. 6
E-mail: murad.mad@outlook.com
ORCID ID: https://orcid.org/0000-0003-3332-2850
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58624042900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/ABB-9737-2021
Google Scholar ID: https://scholar.google.com/citations?user=qpGC84MAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=1212027

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование выполнено за счет гранта Российского научного фонда № 25-28-01478. https://rscf.ru/project/25-28-01478/

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 21 августа 2025 г.
Дата одобрения после рецензирования – 4 сентября 2025 г.
Дата принятия к опубликованию – 20 декабря 2025 г.
Дата онлайн-размещения – 25 декабря 2025 г.

Research article
UDC 34:004:346.6:004.8:347.78
EDN: https://elibrary.ru/xeltpk
DOI: https://doi.org/10.21202/jdtl.2025.24

Copyright Facing the Challenges of Generative Artificial Intelligence: Judicial Practice and Legislative Strategies in India, the United States and the European Union

K. S. Amith Sriram
Ramaiah College of Law, Bengaluru, India

Keywords

artificial intelligence,
blockchain,
comparative legal studies,
copyright,
data analysis,
digital technologies,
generative artificial intelligence,
judicial practice,
law,
legal regulation

Abstract

Objective: to conduct a comparative analysis of the judicial interpretation of the fair dealing and fair use doctrines in the copyright law systems of India, the United States and the European Union in the context of the challenges posed by the development of generative artificial intelligence and blockchain technologies.

Methods: the work uses a set of scientific methods, including a comparative legal analysis of the legislation of three jurisdictions, a systematic analysis of judicial practice in India, a dogmatic method of interpreting regulations, as well as a structural and functional approach to the study of legal institutions. Special attention was paid to over sixty years of Indian judicial practice in applying the fair dealing doctrine, to the American fair use doctrine with its four-factor test, and to the European system of legislative exceptions in text and data mining. The research methodology includes a historical and legal method for identifying evolutionary trends in the judicial interpretation of copyright exceptions, a formal legal method for analyzing the normative content of legal institutions, and a legal modeling method for developing recommendations to improve legislation for regulation of generative artificial intelligence and blockchain technologies.

Results: the study convincingly demonstrates the structural inconsistency of the Indian closed-list system of copyright exclusions for regulating

generative artificial intelligence and blockchain technologies. It was established that the Indian fair dealing doctrine is characterized by five fundamental limitations: excessively literal interpretation of the legislative text, lack of a transformative use concept, inability to adapt to digital formats, legal gap in the regulation of the artificial intelligence outputs, and significantly limited application. A comparative analysis revealed that the American system reaches structural limits when regulating the large-scale use of data, whereas the European model covers the data input but not the commercialization of artificial intelligence outputs.

Scientific novelty: the research presents a comprehensive comparative legal analysis of the application of the fair dealing and fair use doctrines to generative artificial intelligence and blockchain technologies. The study systematizes more than sixty years of judicial practice in three legal systems, which allowed identifying the structural limitations of both open and closed models of copyright exceptions and justifying the need to comprehensively regulate full cycle of the creation and commercialization of artificial intelligence content.

Practical significance: the results can be used to develop national strategies for regulating artificial intelligence; reform the system of copyright exceptions; introduce technologically neutral standards for text and data mining; create disclosure mechanisms for training datasets and registers of copyright holders' opt-outs; and modernize the system of collective rights management using blockchain.

For citation

Amith Sriram, K. S. (2025). Copyright Facing the Challenges of Generative Artificial Intelligence: Judicial Practice and Legislative Strategies in India, the United States and the European Union. *Journal of Digital Technologies and Law, 3*(4), 598–635. https://doi.org/10.21202/jdtl.2025.24

Contents

Introduction

> We shape our tools and thereafter our tools shape us.
>
> **Marshall McLuhan**

With the advent of generative artificial intelligence (GenAI), which represents a paradigm shift in both technological capabilities and normative legal frameworks, this aphorism finds new relevance (Hauck, 2021; Li, 2024; Li & Wang, 2024). GenAI is a class of artificial intelligence systems that can learn patterns from vast amounts of training data to produce novel outputs like text, images, audio, or code on their own. These systems, particularly general-purpose AI models, are self-evolving systems that increasingly mediate the creation, organization, distribution, and monetization of information. They are more than just computational tools. Although human intent shaped their design, capabilities, and applications, their social impact is currently reshaping the limits of ethical responsibility, regulatory design, and intellectual property law (Lund & Samuelson, 2024; Mohammed, 2025; Rosati, 2025a, 2025b).

Since the release of OpenAI's GPT-3 in 2020, the sophistication, scope, and impact of GenAI models have increased significantly[1]. From writing simple prose, these models have developed multimodal fluency in text, image, code, and audio generation. The most recent generation of foundation models, including GPT-4, Claude 3, Gemini 1.5,

[1] OpenAI, GPT-3 Technical Paper. (2020). arXiv:2005.14165.

and Mistral Mixtral, exhibit advanced capabilities in software development, legal summarization, scientific reasoning, and real-time multilingual translation[2]. These models are currently applied in AI tutoring in international universities to court assistance in New York[3]. Tools like Google's AI-integrated Workspace, Adobe Firefly, and Microsoft Copilot have incorporated Gen-AI capabilities into millions of people's productivity workflows[4]. However, these developments have also caused significant disruptions to the established principles of intellectual property law. While producing novel outputs, GenAI uses enormous amounts of training data sets composed of text, photos, audio, and video from online sources. These datasets include creative works authored by individuals, institutions, often without any consent, attribution and regimentation of right holders[5]. This practice raises critical legal question regarding unauthorized reproduction and the scope of permissible use in AI training and deployments (Xie et al., 2024; Yu et al., 2023).

These concerns have already been materialized across jurisdictions including the United States, the United Kingdom, the European Union and India and gave rise to litigations, where copyright holders sued AI developers, claiming infringement in both the training and output stages of generative AI systems. In nearly every instance, the core line of defense or judicial reasoning relied on the fair use doctrine (in the United States), or statutory exceptions and limitations (in Europe and India), to justify the use of copyrighted content in training corpora (Rosati, 2025a, 2025b; Sood, 2024; Volkova, 2021). In New York Times Co v Open AI, Getty Images v Stablity AI, even in ANI v OpenAI in India, the defendant claimed that their use to train large language models (LLMs) falls under the exceptions of Copyright Act[6].

This series of litigations reveals the pivotal role that copyright exception frameworks play in the generative AI ecosystem. The United States has a flexible fair use doctrine under 17 U.S.C. § 107 that allows courts to determine whether uses of copyrighted content, like algorithmic training, are allowed based on factors like purpose, nature, amount, and market effect[7]. U.S courts upheld such uses in Authors Guild v. Google Inc. Sega Enters.

---

2 OpenAI, GPT-4 Technical Report. (2023). arXiv:2303.08774; Anthropic, Claude 3 Model Card. (2024).

3 Microsoft, Copilot Overview. (2024); NYSBA, AI Legal Pilot. (2025); ETH Zurich & University of Tokyo, Academic AI Report. (2025).

4 Microsoft, Copilot Product Overview. (2024); Adobe, Firefly White Paper. (2024).

5 European Parliament. (2025, January). Generative AI and Copyright: Training, Creation, Regulation, PE 774.095 (pp. 10–13).

6 The New York Times Co. v. OpenAI, Case No. 1:23-cv-11195 (S.D.N.Y. 2023); Getty Images v. Stability AI, [2023] EWHC 2333 (Ch).; ANI Media v. OpenAI, pending before Delhi High Court. (2024).

7 17 U.S.C. § 107. (2012).

Ltd. v. Accolade, Inc., and even in recent Bartz v. Anthropic[8]. Similarly, the European Union has modernized its copyright laws with Directive (EU) 2019/790, which added distinctive text and data mining (TDM) exceptions under Articles 3 and 4 to support AI development[9]. However, under Section 52 of the Copyright Act, 1957, India maintains a closed-list system of exceptions that only allow fair dealing for specific uses, such as private use, research, criticism, and reporting on current events, with no recognition of TDM or AI training uses[10].

Even if Gen-AI use of copyrighted content during the training phase is considered permissible, the output stage raises distinct challenges, especially when the content is created as digital artworks or deployed within distributed ledger technologies (Buick, 2025; Chauhan, 2025; Chopra, 2025; Dornis, 2025; Grodzinsky et al., 2007). GenAI outputs that closely resemble protected characters or styles can give rise to direct copyright claims, as demonstrated by recent cases such as Disney v. Midjourney[11]. These instances clearly indicate that the focus of litigation has shifted from the training phase to the nature and legality of the outputs. As generative models are more capable of replicating the distinctive elements, the evaluation of output-stage infringement is evolving from a peripheral concern to a central legal challenge. Therefore, in the GenAI era, the output stage is becoming a growing focus of copyright enforcement rather than a theoretical issue. Figure 1 below indicates this shift, showing how Midjourney's output resembles the visual identity of Disney's Elsa.

Figure 1. Visual comparison of Midjourney's output (left) and Disney's copyrighted character Elsa (right)[12]

8 Authors Guild v. Google Inc., 804 F.3d 202, 219–25 (2d Cir. 2015); Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1523–27 (9th Cir. 1992); Bartz v. Anthropic PBC, No. 3:23-cv-05867 (N.D. Cal. filed Nov. 14, 2023).

9 Directive (EU) 2019/790, arts. 3–4; see also European Parliament, Generative AI and Copyright: Training, Creation, Regulation, PE 774.095 (2025, January), at 14–18.

10 The Copyright Act, 1957, § 52, No. 14, Acts of Parliament, 1957 (India).

11 Disney Enters., Inc. v. Midjourney, Inc., No. 2:25-cv-05275 (C.D. Cal. filed June 11, 2025).

12 The Walt Disney Co. and Universal City Studios LLC, Hollywood Strikes Back: Disney and Universal Sue AI Platform Midjourney for Copyright Infringement. (2025, June 25). Mondaq. https://clck.ru/3Qsv3d

This research paper argues that India's closed-list fair dealing provision lacks potential to regulate generative AI systems and blockchain-based assets. It draws on structured judicial mapping of Indian fair dealing decisions from 1959 to 2025 to identify long-term patterns in which courts have construed copyright exceptions across different technologies. This analysis demonstrates that the problem is not merely an inconsistent judicial interpretation but a statutory rigidity that limits juridical adaptability in the face of emerging technologies.

By placing this mapping within a comparative framework, the paper analyzes the more flexible U.S. fair use doctrine and the developing statutory exception regime of the European Union under the DSM Directive. While the U.S. and EU frameworks are more flexible, the study finds that both remain structurally insufficient to adequately handle the legal complexities brought about by GenAI, especially when it comes to issues like the use of large amounts of training data, attribution of generated content, and the uniqueness of outputs produced by AI. In contrast, India's exception lacks transformative or output-focused reasoning and is purpose-bound, making it even less capable of addressing these developments.

To address these challenges, this paper presents a set of context-specific reform proposals that are intended to be in line with India's unique legal system and technological environment. These proposals include opt-out procedures, statutory licensing models, and an extension of public interest-based exceptions. Given the recent establishment of an expert committee on generative AI and copyright law by the Indian government following the interim proceedings in ANI Media Pvt. Ltd. v. OpenAI Inc. (Delhi High Court, 2024)[13], these proposals become even more pertinent.

Similar to Volvo's 1959 decisions to open up its three-point seatbelt patent for public use in the interest of safety[14], copyright holders should consider permitting limited use of their works for AI training, with appropriate safeguards. This study suggests compensation models, such as opt-out procedures and statutory licensing, to assist India in creating a fair and modern copyright framework.

[13] Government of India. (2025). Constitution of Expert Committee on Generative AI and Copyright Law, Ministry of Electronics and Information Technology (following interim proceedings in ANI Media Pvt. Ltd. v. OpenAI Inc., Delhi High Court, C.S. (COMM) 97/2024).

[14] Volvo Cars, The Story of the Three-Point Seat Belt. (1959).

1. Judicial interpretation of fair dealing in India (1959–2025)

Over 60 years of judicial interpretation of Section 52 of the Copyright Act, 1957, reveals a structurally inflexible jurisprudence. India's fair dealing exception (Section 52(1)(a)) operates on a closed-list basis, restricted to specific uses like private study, criticism, review, research, and current event reporting. This section argues that the limitations in Indian fair dealing law stem not from unpredictable judicial interpretation, but from the restrictive architecture of the statute itself. This paper highlights five major trends demonstrating the statute's incapacity to support emerging technologies, such as generative AI and blockchain-based creativity, drawing on 19 decisions rendered between 1959 and 2025 (for a detailed chronological mapping of these cases, see Table in the Appendix)[15].

1.1. Limited scope of fair dealing and judicial restraint

Consistent judicial restraint in India is demonstrated by strict adherence to the specific categories listed in Section 52(1)(a), which essentially prevents judicial expansion into related or developing uses. The early decision in Blackwood & Sons Ltd. v. A.N. Parasuraman, which severely limited reproduction to private study, is a clear example of this interpretive approach[16]. This strict construction continued to shape later decisions, like the Delhi High Court's decisions in Super Cassettes v. Hamar Television and Yashraj Films v. RK Productions. Despite their potential informational or public interest components, the courts in both cases interpreted the term "reporting current events" so narrowly that they disregarded media such as musical interludes in talk shows and TV shows[17]. This collective jurisprudence highlights a judicial reluctance to infer broader legislative intent beyond the text, thus creating a statutory bottleneck for unforeseen technological applications.

The judiciary itself has acknowledged this interpretive restraint. The Court acknowledged in NDTV v. ICC that any extension of the particular fair dealing purposes listed in Section 52(1)(a) requires legislative authority[18]. Similarly, the Delhi High Court acknowledged the statute's functional limitations in Rameshwari Photocopy, although with some leeway for educational access.

---

15 For detailed case information, see Table 1 in the Appendix.

16 Blackwood & Sons Ltd. v. A.N. Parasuraman, AIR 1959 Mad. 410 (India)

17 Super Cassettes Indus. Ltd. v. Hamar Television Network Pvt. Ltd., 2010 SCC OnLine Del 2402; Yashraj Films Pvt. Ltd. v. RK Productions, 2012 SCC OnLine Del 1112.

18 NDTV v. ICC Dev. (Int'l) Ltd., 2012 SCC OnLine Del 4812, para 19.

1.2. The lack of transformative use

The lack of a transformative use framework is a persistent gap in Indian fair dealing. While U.S. jurisprudence assesses whether a secondary use fundamentally alters the original's intent or character, Indian courts remain anchored to a narrow consideration of whether the use falls strictly within the enumerated statutory purposes. For instance, in Civic Chandran v. Ammini Amma, while protecting a counter play for its critical stance, the Kerala High Court framed its reasoning around ideological intent rather than transformative expression[19]. This narrow focus was further exemplified by the Bombay High Court in Shemaroo Entertainment Ltd. v. News Nation, which refused to examine whether using archival film clips in a political show served any additional purpose[20]. Consequently, without a tranformativeness standard, Indian law cannot accommodate uses where AI systems remix or reinterpret original works to produce something substantially new (Al-Busaidi, 2024; Balganesh, 2013, 2017; Bonadio & McDonagh, 2025).

1.3. Lack of adaptability to evolving formats and digital platforms

Indian courts have consistently struggled to reconcile fair dealing with digital platforms and new content formats. This difficulty is exemplified by the Delhi High Court ruling in MySpace v. Super Cassettes, which held that the platform was accountable for user-uploaded content, disregarding algorithmic distribution as either transformative or passive[21]. Subsequent decisions, such as Star India v. Piyush Agarwal (live tweeting of cricket score) and Tips v. Wynk Music (streaming vs broadcasting), further reinforced a limited understanding of current licensing categories and technological equivalency, disqualifying new digital uses. Together, these decisions show how the strict statutory language hinders judges' ability to adjust to the emerging digital landscape[22]. Importantly, this interpretive position implies that web-hosted data that is necessary for training generative AI systems is unlikely to be deemed legally acceptable under the current fair dealing standards in India. This effectively ignores crucial platform-based data ingestion and remix models, even for non-commercial or culturally significant uses.

---

19 Civic Chandran v. Ammini Amma, 1996 SCC OnLine Ker 417; AIR 1996 Ker 291.

20 Shemaroo Ent. Ltd. v. News Nation Network Pvt. Ltd., 2022 SCC OnLine Bom 930.

21 MySpace Inc. v. Super Cassettes Indus. Ltd., 2016 SCC OnLine Del 6386.

22 Star India Pvt. Ltd. v. Piyush Agarwal, 2013 SCC OnLine Del 1469; Tips Indus. Ltd. v. Wynk Music Ltd., 2019 SCC OnLine Bom 13063, paras.

1.4. Silence on output-stage infringement and AI generated authorship

The issue of whether AI-generated content could be considered infringement in and of itself has not yet been directly addressed by Indian copyright jurisprudence. The Delhi High Court considered whether teaching LLMs about news articles in ANI v. OpenAI infringed copyright, but it has not yet made a decision regarding the implications for the output stage[23].

When AI outputs mimic or synthesize protected styles, this silence is concerning. Courts in the United States are currently debating whether AI outputs that closely mimic or replicate copyrighted content may give rise to liability in cases like Authors Guild v. OpenAI, Tremblay v. OpenAI, and Universal Music v. Anthropic[24]. There is no doctrinal guidance in Indian law to differentiate between acceptable synthesis and prohibited replication. Indian courts will probably not be able to handle new issues pertaining to AI-generated art, or deepfake-style content without legislative change.

1.5. Limited engagement with comparative fair use doctrine

Indian courts have occasionally looked at fair use or fairness standards from other countries. For instance, the U.K. ruling in Hubbard v. Vosper and the U.S. "four-factor test" were mentioned by courts in Super Cassettes, NDTV, and Gallata Media[25]. However, these were only used as helpful guides, not as legally binding rules. Even in cases involving advanced technologies or international companies, Indian courts must stick to the exact wording of Section 52, as the Delhi High Court confirmed in ANI v. OpenAI.

Even though this comparative caution is in line with long-standing Indian legal principles, it actually makes the current statutory framework even more restrictive. Therefore, India's legal system runs the risk of becoming stagnant as other jurisdictions broaden the definition of fair use or enact particular exemptions for artificial intelligence, making it more difficult for the country to keep up with the latest developments in both domestic and foreign technology.

---

23 ANI Media Pvt. Ltd. v. OpenAI Inc., CS(COMM) 1028/2024 (Del HC, pending), interim proceedings.

24 Authors Guild v. OpenAI, Inc., No. 1:23-cv-08292 (S.D.N.Y. filed Sept. 2023), Compl.Tremblay v. OpenAI, Inc., No. 4:23-cv-03223 (N.D. Cal. filed June 2023), Compl. Universal Music Publ'g Grp. v. Anthropic PBC, No. 3:23-cv-01092 (C.D. Cal. filed Oct. 2023).

25 Gallata Media Pvt. Ltd. v. Union of India, 2024 SCC OnLine Del 452.

2. Comparative analysis of copyright exceptions in the U.S. and the EU

The structural limitations of Section 52 of the Indian Copyright Act, 1957, emphasized in the preceding analysis, make it necessary to look at how other jurisdictions have handled limitations and exceptions in the face of technological disruption. The United States and European Union offers two significant and divergent approaches regulating relationship between copyright and innovation. The U.S. fair use doctrine, primarily judge-made and open-ended, is characterized by its adaptability and contextual balancing of interests. In contrast, the EU framework is more codified, rooted in directive-based harmonization and specific statutory exceptions, including provisions for text and data mining under Directive (EU) 2019/790[26]. Currently, both systems are under pressure to address the legal ambiguity surrounding blockchain-based assets and generative AI. Regarding AI training and dissemination, courts and policymakers in these jurisdictions are debating issues of scope, permissibility, and compensation with conflicting outcomes[27].

By analyzing the legal reasoning, statutory developments, and emerging responses in both the U.S. and the EU, this section critically evaluates how various exception regimes are accommodating or failing to accommodate demands of the generative AI and blockchain-driven creative economy.

2.1. Fair use in United States

The United States' fair use doctrine, codified in 17 U.S.C. § 107, is an open-ended exception to copyright infringement that permits limited uses of copyrighted content without prior consent. It contrasts with the European Union's directive-based statutory exceptions and India's closed-list model under Section 52.

U. S. Court assesses fair use by applying a four-factor test:

(1) the purpose and character of the use, including whether it is transformative;

(2) the nature of the copyrighted work;

(3) the amount and substantial portion used; and

(4) the effect of the use upon the potential market for the original work[28].

---

[26] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market, 2019 O.J. (L 130) 92.

[27] See, e.g., Andersen v. Stability AI Ltd., No. 3:23-cv-00201 (N.D. Cal. filed Jan. 13, 2023); European Copyright Society, Generative AI and Copyright Law: A Position Paper, (Feb. 2024). https://clck.ru/3QsxbW

[28] 17 U.S.C. § 107 (2012).

Although courts consider all four factors, contemporary jurisprudence has increasingly prioritized the first one, particularly the notion of transformativeness, as central to the fair use analysis. While the four factors are statutorily enumerated, the fair use doctrine has evolved through judicial interpretation with minimal legislative intervention. The modern fair use analysis is based on the concept of transformativeness, which was explicitly stated by the U.S. Supreme Court in Campbell v. Acuff-Rose Music, Inc.[29]

Fair use has exhibited notable adaptability in responding to technological change, owing to its open-text statutory language, which affords courts the necessary interpretive latitude to assess novel uses on a case-specific basis. One of the earliest cases that demonstrates such judicial engagement was Sony Corp. of America v. Universal City Studios, Inc.[30] In it, the U.S. Supreme Court ruled that the use of videocassette recorders (VCRs) for time-shifting television broadcasts qualified as fair use. The court emphasized the value of technological innovation in the face of strict copyright enforcement and stressed that private, non-commercial copying for later viewing did not reduce the market for the original work. This reasoning was expanded by the Ninth Circuit in Sega Enterprises Ltd. v. Accolade, Inc., where the court held that reverse engineering copyrighted code to gain access to unprotected functional elements constituted fair use, as it encouraged market competition and interoperability in the software sector[31].

In contrast to the closed-list system, fair use's flexibility has continuously provided judges with the ability respond to evolving technologies. In Campbell v. Acuff-Rose Music, Inc.[32], the Supreme Court identified transformativeness as the primary issue, stating that a use can be considered fair even if it is commercial as long as it adds new expression, meaning, or message. This notion of transformativeness evolved into a crucial analytical tool for evaluating new applications pertaining to software and the digital world. Similarly, in Kelly v. Arriba Soft Corp., the United States Court of Appeals for the Ninth Circuit held that, a search engine's production and display of smaller "thumbnail" images amounted to highly transformative use, because it made indexing and retrieval easier, which was completely different from the expressive intent of the original photos[33]. This reasoning was reaffirmed in Perfect 10, Inc. v. Amazon.com, Inc., where it was held that Google's creation of low-resolution thumbnail images of copyrighted photos for its search results served

29 Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994).

30 Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 447–56 (1984).

31 Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992).

32 Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994).

33 Kelly v. Arriba Soft Corp., 336 F.3d 811, 818–22 (9th Cir. 2003).

a novel and distinct purpose rather than reproducing the original aesthetic or commercial value of the image. Accordingly, the production and presentation of thumbnails qualified as fair use under 17 U.S.C. §107[34].

Fair use doctrine continued to evolve as courts addressed increasingly complex digital use case. The Second Circuit upheld the mass digitization of millions of books for the Google Books project in Authors Guild, Inc. v. Google, Inc., concluding that displaying a small number of book excerpts and establishing a full-text searchable database was a distinctly transformative use that promoted public research and discovery without replacing the original market[35]. By imposing an affirmative duty on copyright holders to consider potential fair use before issuing DMCA takedown notices, the Ninth Circuit further expanded fair use protections in Lenz v. Universal Music Corp., building on this digital context and protecting legitimate user-generated content on online platforms[36]. The application of fair use to evolving technologies was reaffirmed in Supreme Court's decision in Google LLC v. Oracle America, Inc., where court held that Google's reimplementation of Oracle's Java API declaring code for the Android platform was revolutionary since it allowed for the creation of a completely new software environment for mobile devices[37]. These decisions illustrate a consistently evolving judicial approach to fair use, marked by a positive interpretation that evolves with technology and gives transformative public benefit precedence over rigid reproduction-based restrictions.

However, the emergence of generative AI and blokchain-based assets has posed unprecedented challenges, testing the scope of fair use. In Bartz v. Anthropic PBC and Kadrey v. Meta Platforms[38], Inc., the Northern District Court of California for the very first time in the world determined that using copyrighted works to train large language models constituted fair use because machine learning goal and output (producing statistical models of language) are essentially different from expressive and creative objectives of the original works[39]. Despite these decisions, boundaries of fair use remain unsettled. A growing wave of disputes such as Silverman v. OpenAI, Inc., Tremblay v. OpenAI, Inc., Doe v. GitHub, Inc., Andersen v. Stability AI Ltd. and other pending cases continues to challenge the fair use doctrine. In each of these cases, the defendants consistently argue that their

34 Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1165–68 (9th Cir. 2007).

35 Authors Guild v. Google, Inc., 804 F.3d 202, 214–25 (2d Cir. 2015).

36 Lenz v. Universal Music Corp., 815 F.3d 1145, 1153–55 (9th Cir. 2016).

37 Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183, 1202–10 (2021).

38 The organization is recognized as extremist, its functioning is prohibited in the territory of the Russian Federation.

39 Bartz v. Anthropic PBC, No. 3:23-cv-03122, slip op. at 12–18 (N.D. Cal. June 23, 2025); Kadrey v. Meta Platforms*, Inc., No. 3:23-cv-04744, slip op. at 8–15 (N.D. Cal. June 25, 2025). (* The organization is recognized as extremist, its functioning is prohibited in the territory of the Russian Federation.).

systems' outputs are the product of essentially distinct computational processes rather than derivative works[40].

These lawsuits focus in their initial rulings predominately on the input stage, particularly the use of copyrighted material for model training, while paying limited attention to output uses of generated content and commercialization through digital outputs. The controversy surrounding Zarya of the Dawn, a comic book with AI-generated illustrations, raised concerns about the potential for unapproved replication of AI-generated (and thus potentially uncopyrightable) styles or likenesses. Complaint allegations in Andersen v. Stability AI clearly illustrate the growing concern over output-stage uses of generative AI and the commercialization of such content[41]. Commercializing generated outputs transforms them into monetizable digital assets with commercial intent. When fair use arguments and analysis are framed around the input stage, the legal status of inputs and the subsequent commercialization of outputs remain unsettled.

Large-scale commercial AI training and the expressive, high-fidelity pushes fair use beyond its traditional limits. Earlier decisions such as Sony, Sega, Google Books, and Oracle showed how flexible fair use could be to new technological developments, but they were mostly limited to specific, intermediate features like allowing software interoperability, time shifting for private viewing, or developing searchable indexes and snippet displays to make information discovery easier. In contrast to the mass consumption, internalization, and recombination of creative expression, these cases involved ancillary, non-expressive uses.

Copyright has been established to control individual instances of illegal use or copying. However, generative models do not replicate recognizable works directly; instead, they extract and synthesize patterns from large datasets. As a result, conventional copyright systems designed to regulate individual reproductions find it difficult to handle this use of aggregate, pattern-based data. The emergence of so-called "commercially safe" systems, like Getty Images' diffusion-based AI platform and Adobe's Firefly, that are trained solely on licensed or owned datasets, makes this limitation clear[42]. Due to their avoidance of unlicensed scraping, these models are completely exempt from the usual

---

40 See Silverman v. OpenAI, Inc., No. 3:23-cv-03416, 2023 WL 4824158 (N.D. Cal. filed July 7, 2023); Tremblay v. OpenAI, Inc., No. 3:23-cv-03223, 2023 WL 4824145 (N.D. Cal. filed June 28, 2023); Doe v. GitHub, Inc., No. 4:22-cv-06823, 2022 WL 16840396 (N.D. Cal. filed Nov. 3, 2022); Andersen v. Stability AI Ltd., No. 3:23-cv-00201, 2023 WL 7132064 (N.D. Cal. filed Jan. 13, 2023).

41 See Andersen complaint para (67–72); Medium, "Artificial Intelligence, NFTs & Copyright: Can AI-Generated Art be Copyrightable?" (2023, June 27).

42 Weatherbed, J. (2023, May 23). Adobe Is Adding AI Image Generator Firefly to Photoshop. The Verge.

infringement claims. Yet they continue to produce low-cost, adaptable, and stylistically accurate products that undermine established markets and replace human creative labor. This shows that the wider structural and economic harms posed by generative AI cannot be addressed by copyright, which is intended to control specific instances of unlawful copying.

In light of aforementioned analysis, the development of U.S. fair use indicates its flexibility to technological change, from search engines and VCRs to mass digitization and software interoperability. However, generative AI pushes fair use to the very edge of its doctrinal bounds by introducing unprecedented large-scale, high-fidelity uses that internalize and recombine creative expression without direct reproduction. The inability of copyright to address the wider economic and systemic harms of generative technologies is revealed by the fact that even "commercially safe" models trained only on licensed datasets can displace human labor and disrupt creative markets without giving rise to traditional infringement claims.

Courts in the United States have evaluated the fourth factor under 17 U.S.C. § 107 (effect on the market) through the lens of direct substitution or measurable license revenue loss. Cases like Harper & Row v. Nation Enterprises and American Geophysical Union v. Texaco, clearly indicate this approach, finding market harm where unauthorized use disrupted existing licensing agreements[43]. However, generative AI introduces a qualitatively distinct kind of market interference. These systems absorb and recombine expressive content at scale instead of reproducing or disseminating preexisting works, which causes enormous economic displacement in the creative industries. The rise of "commercially safe" models that are only trained on licensed or proprietary datasets indicates this. Even in the absence of infringement, such models can erode demand for human-created content, exposing copyright's inability to address systemic disruption that occurs without unauthorized copying.

While courts in cases like Bartz v. Anthropic have suggested that using legally obtained books for training may be considered fair use[44], this reasoning avoids the issue of whether it should be acceptable to consume expressive works in large quantities and without consent just because no direct reproduction takes place. The fair use test also lacks the potential to address the compensation crisis posed by GenAI. The microscopic

[43] Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 566 (1985): Am. Geophysical Union v. Texaco Inc., 60 F.3d 913, 929 (2d Cir. 1994).

[44] Bartz, No. 3:23-cv-05867.

contribution of each individual work in model training makes proposals for licensing or compensation, like collective management or opt-out mechanisms, practically untenable.

A comparable challenge arises with the commercialization of generative AI outputs, especially when integrated with distributed ledger technologies, which puts additional pressure on the limits of fair use. Despite calls to expand fair use in virtual environments to foster creativity, the legal status of novel digital content remains unsettled. Policy commentary has emphasized the need for additional case law to clarify how fair use and First Amendment defenses apply to digitally distributed content[45].

The limitation of fair use is even more evident in the context of generative AI. The U.S. Copyright Office has explicitly observed that the current framework is "not well-suited to address the kinds of uses at issue in generative AI training" and that "fair use was developed for individualized, case-by-case application", making it challenging to scale to the automated, aggregate ingestion of millions of works[46]. Similarly, Judge Araceli Martínez-Olguín recognized the doctrinal strain imposed by GenAI in Andersen v. Stability AI, noting that "traditional infringement doctrines may not adequately capture the diffuse harms caused by AI training processes that do not replicate content in the conventional sense"[47].

Despite its historical flexibility in adapting to emerging technologies, the fair use doctrine is now confronting the outer limits of its normative design, not due to judicial misapplication, but because it was never conceived to regulate generative processes that blur the distinction between transformation and replication at scale.

2.2. Copyright exceptions in the European Union

Unlike the Unites States open-ended fair use model, EU adheres to a closed-list, statutory model for copyright exceptions. This framework was codified in Directive 2001/29/EC (the "InfoSoc Directive") and further updated through Directive (EU) 2019/790 (Digital Single Market Directive). A comprehensive list of permissible exclusions and limitations is provided under Article 5(1)–(3) of the InfoSoc Directive[48]. All exceptions are additionally subject to the three-step test outlined in Article 5(5), which states that an exception must: (i) only be applicable in specific special circumstances, (ii) not interfere

45 U.S. Copyright Office & U.S. Patent & Trademark Office, NFTs, Copyright, and Intellectual Property (2023, July).

46 U.S. Copyright Office, Copyright and Artificial Intelligence: Notice of Inquiry, 88 Fed. Reg. 51389, 51391 (2023, Aug. 3).

47 Andersen v. Stability AI Ltd., No. 3:23-cv-00201, Transcript of Proceedings at 34 (N.D. Cal. May 3, 2024).

48 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, pp. 10–19, Art. 5(1)–(3).

with the work's regular exploitation, and (iii) not unreasonably jeopardize the rights holder's legitimate interests[49].

While this statutory model maintains a closed list, courts have applied three-factor test to interpret copyright exceptions and accommodate digital technologies. In Football Association Premier League v QC Leisure, confirming that temporary technical reproductions, including on-screen display and browser caching satisfies three-factor test, Court upheld its legality[50]. Similarly in hyperlinking cases like Svensson v. Retriever Sverige AB and GS Media v. Sanoma Media Netherlands, CJEU ruled that hyperlinking to publicly accessible works does not qualify as "communication to the public" when it fails to meet essential components of the three-factor test[51]. However, the digital uses such as text and data mining and large-scale digitization outpaced the interpretative potential; the European Commission formally recognized this short fall in its 2016 impact assessment, identifying it as a barrier to innovation and cross-border research[52].

In response to this, DSM Directive was enacted, with several new mandatory exceptions such as text and data mining (TDM) (which allows computers to analyze large volumes of text and data for research or commercial use, unless right holders expressly reserved their rights)[53], digital teaching (which allows educators to use copyrighted content for online and cross-broader teachings)[54], and cultural heritage preservation (which allows libraries and archives to reproduce copyrighted work solely for the purpose of long term preservation)[55].

Following the DSM Directive, the European Union passed the Artificial Intelligence Act in response to the rapid growth of generative AI technologies, especially to address the large language models' (LLMs') complex output production capabilities[56]. This act mandates the providers of general-purpose AI (GPAI) models to adopt a copyright compliance policy and to publish detailed summaries of training data, specifically identifying any rights-holder opt-outs[57]. In Recital 105, the Act clarifies that training an AI model using copyrighted

---

49 Ibid, Art. 5(5).

50 Football Ass'n Premier League v. QC Leisure, Case C-403/08, 2011 E.C.R. I-9079.

51 Svensson v. Retriever Sverige AB, Case C-466/12, 2014 E.C.R. I-0000; GS Media v. Sanoma Media Netherlands, Case C-160/15, 2016 E.C.R. I-0000.

52 Commission Staff Working Document, Impact Assessment on the Modernisation of EU Copyright Rules, SWD (2016) 301 final (Sept. 14, 2016).

53 Directive (EU) 2019/790, Articles 3–4, on copyright and related rights in the Digital Single Market, OJ L 130, 17.5.2019, pp. 92–125.

54 Ibid, Article 5.

55 Ibid, Article 6

56 Waem, H., & Deircan, M. (2023, Nov. 13). A Deeper Look into the EU AI Act Trilogues: Fundamental Rights Impact Assessments, Generative AI and a European AI Office. Kluwer Competition Blog. https://clck.ru/3Qsxe4

57 Artificial Intelligence Act (Regulation 2024/1689), art. 53(5); Directive (EU) 2019/790, art. 4(3), on copyright and related rights in the Digital Single Market, OJ L 130, 17.5.2019, pp. 92–125.

material, even outside the EU, must comply with TDM rules, and that silence from rights holders does not equal consent[58]. These transparent obligations enable AI developers to establish lawful reliance on the TDM exception in court, thereby reinforcing it as a viable legal defense.

As of July 2025, the Court of Justice of the European Union (CJEU) has not made a decision that specifically addresses whether generative AI systems' output or training phases are protected by Articles 3 or 4 of the DSM Directive. A conclusive court interpretation is still pending, despite the pending case like Company v. Google Ireland[59]. Despite these legislative developments in EU, the TDM exceptions outlined in Articles 3 and 4 of the DSM Directive remain limited in their applicability to generative AI[60]. A closer analysis of the legal framework indicates these clauses were not intended for the broad and expressive characteristics of general-purpose AI models, but rather for specific, limited-use cases, mainly data analytics for scientific research and low-risk commercial applications. While Article 3 focuses on non-commercial scientific research, Article 4 allows limited commercial uses with tight restrictions. The opt-out mechanism allows right holders to exclude their work from being used by deploying "machine-readable means," signals such as robots.txt. In practice, this means the publicly available content cannot be lawfully used for training generative AI if right holders have issued such exclusions. The output stage of generative AI, or the reuse, replication, or public dissemination of AI-generated content derived from copyrighted materials, is not expressly permitted or regulated by any corresponding exception under EU law.

These exceptions fail to address the issues of outputs; the scope of these exceptions is limited to input stage of AI development, which is the ingestion and analysis of datasets. In addition to being analytical tools, generative models are made to internalize patterns, replicate style, and produce high-fidelity content that frequently mimics expressive aspects of works protected by copyright. This limitation is evident in several cases. Stability AI's Stable Diffusion and OpenAI's DALL-E have generated outputs that closely mimic the visual styles of copyrighted artists, including Greg Rutkowski, whose name was commonly used in image-generation prompts. These results are not ambiguous derivatives; rather, they frequently mimic unique visual characteristics that are essential to the original works'

58 Artificial Intelligence Act (Regulation 2024/1689), Recital 105.

59 Like Company v. Google Ireland, Case C-250/25, request for preliminary ruling from Fővárosi Törvényszék (Budapest Metropolitan Court), filed Apr. 2025; see also "CJEU to Rule on AI and Copyright in Landmark Case Against Google," Stephenson Harwood Technology Insight (2025, Apr.). https://clck.ru/3Qsvhr

60 Directive (EU) 2019/790, arts. 3–4; European Copyright Society, Generative AI and Copyright: Training, Creation, Regulation, PE 774.095 (2025, Jan.), at 22–23.

identity. Figures 2 and 3 below show how a prompt that invokes Rutkowski's style produces visual outputs that closely resemble the aesthetic qualities of his original works[61].

Figure 2. Original artwork by Greg Rutkowski: this picture exemplifies Rutkowski's unique aesthetics, which is distinguished by dramatic lighting, dynamic fantasy compositions, and fine texture details

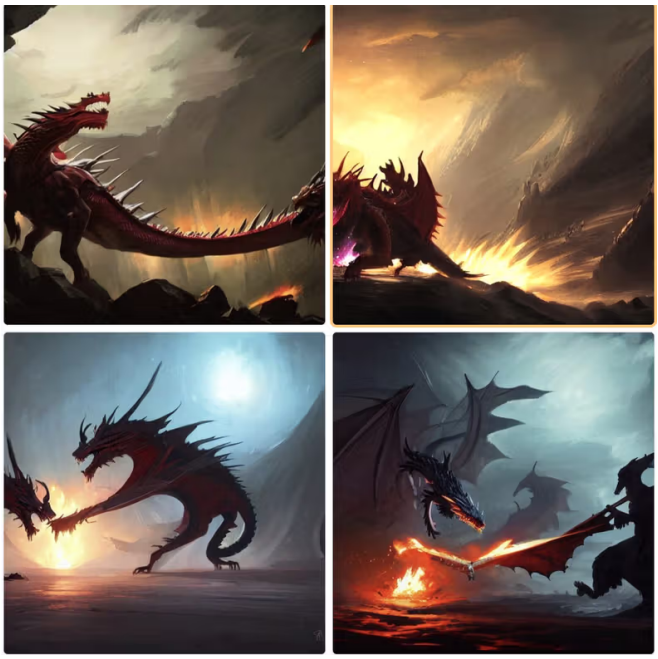


Figure 3. Image poroduced by AI "in the style of Greg Rutkowski". A text prompt that specifically invoked Rutkowski's name in a generative model (such as Stable Diffusion) produced this image.

Such uses raises concerns about the originality, expressive appropriation, and the boundaries of copyright exceptions. The DSM Directive does not clarify whether such outputs fall within the scope of permissible use, leaving a significant regulatory gap and exposing developers and downstream users to infringement risks.

61 Rutkowski, G. (2022). Fantasy Artwork, Sideshow Blog. https://clck.ru/3QsxmM; Lexica, AI-generated Image in the Style of Greg Rutkowski. https://clck.ru/3Qsvna

This ambiguity extends to the ethos of AI-generated content, particularly when using distributed ledger technologies. Following complaints by European artists regarding the commercial utilization of their artistic styles roughly generated without authorization, The European Union Intellectual Property Office (EUIPO) noted increasing concern over the unauthorized use of artistic style in AI-generated content. While developers and markets have used the exceptions for text and data mining (TDM) extensions through Articles 3 and 4 of the Directive on Copyright in the Digital Single Market (DSM Directive) to endorse upstream data uses, the exceptions were simply never intended to be extended to fixation, public communication, and distribution of outputs, for example, digital artworks or AI-rendered visual media[62]. These uses might fall outside of typical TDM expectations, because the creation and effects likely interfere with the regular use of the underlying work and would cause degrees of harm under the third prong of the international three-factor test. Moreover, more recent decisions in Europe determined that fair-dealing-type defenses do not extend to using AI to duplicate a visual work of art and then distributing it, as this is itself held to be illegal public communication and reproduction[63]. Lastly, the commercialization of AI-generated and recontextualized content on blockchain platforms emphasizes an important disparity between the closed-list, input-based exceptions under the EU and the life cycle of generating content with generative AI and blockchain. Such commercialization introduces a kind of public dissemination and economic fixation beyond what is permitted under the DSM's TDM regime.

In addition to the DSM Directive, the AI Act (Regulation (EU) 2024/1689) imposes binding obligations on general purpose AI providers (GPAI), particularly concerning technical compliance, transparency, and documentation, especially with regard to machine-readable opt-out signals such as those found in robots.txt files[64]. These statutory obligations are reinforced by recent soft-law documents. In July 2025, the European Commission published the General-Purpose AI Code of Practice. It is non-binding but directs GPAI providers to minimize memorization risks, refrain from scraping from piracy domains, and set up easily accessible channels for right holders

62 European Writers' Council et al., Joint Letter to the European Parliament: Protecting the Rights of Creators and Artists vs Generative AI (2025, June 19). https://clck.ru/3Qsvsf; European Union Intellectual Property Office, Development of Generative Artificial Intelligence from a Copyright Perspective (2025). https://clck.ru/3Qsvtw

63 Punto FA S.L. v. VEGAP, Juzgado Mercantil No. 11 de Barcelona, Judgment No. 102/2024 (2024, Apr. 3) (Spain).

64 Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence (AI Act), 2024 O.J. (L 213) 1, arts. 50, rec. 133–137.

to file complaints[65]. Since its publication, the Code of Practice has been endorsed and is being operationalized by several GPAI developers including OpenAI, Microsoft, Alphabet (Google), Anthropic, and Mistral[66].

Subsequently, pursuant to Article 53(1)(d) of the AI Act, the Commission published a mandatory disclosure template. This enforceable document requires GPAI providers to make structured summaries of their training data available to the public kinds and sources of information utilized, if any DSM Directive Article 4 opt-outs were respected, and additional metadata necessary for copyright accountability[67].

Additionally, as stated in Article 50 and Recitals 133–137 of the AI Act, it requires that watermarking be used for synthetic content. These tools work together to offer an operational compliance framework that improves the enforce ability of the few exceptions allowed by the DSM Directive, particularly with regard to text and data mining (TDM).

However, these obligations are procedural rather than substantive; they govern how legal activities must be carried out but do not allow for unlawful uses[68]. Acts of text and data mining that are not covered by Articles 3 and 4 of the DSM Directive cannot be retrospectively validated by compliance with transparency duties or datasets documentation. Notably, rights holders can use machine-readable opt-outs to exclude their works under Article 4(3). Even complete compliance with the AI Act or the General-Purpose AI Code of Practice does not permit the use of those works for training in cases where such exclusions are applicable.

The three-step test codified in Article 5(5) of the InfoSoc Directive continues to shape the structure of EU copyright law[69]. While it serves as a safeguard to guarantee that copyright exceptions are applied narrowly, the test's structure is not capable of addressing high-volume expressive AI-outputs. In instances where AI systems consume millions of diverse works at scale, without focusing on any specific genre or rights holder group, it is challenging to meet the requirement that exceptions only apply to certain special

---

65 European Commission, General-Purpose AI Code of Practice (2025, July 10). https://clck.ru/3QsxnW

66 Anthropic, Anthropic Signs EU Code of Practice on General Purpose AI, (July 10, 2025). https://clck.ru/3Qsvyx; The Indian Express, Microsoft Likely to Sign EU AI Code of Practice, Meta Rebuffs Guidelines. (2025, July 12). (* The organization is recognized as extremist, its functioning is prohibited in the territory of the Russian Federation). https://clck.ru/3QsxoG

67 European Commission, Explanatory Notice and Template for the Public Summary of Training Content Required by Article 53(1)(d) of Regulation (EU) 2024/1689, C(2025) 5235 final (2025, July 24).

68 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market (DSM Directive), 2019 O.J. (L 130) 92, art. 4(3).

69 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (InfoSoc Directive), art. 5(5), 2001 O.J. (L 167) 10.

cases. Additionally, the lack of remuneration or attribution to rights holders creates an imbalance that may "unreasonably prejudice" their legitimate interests.

Therefore, while the EU copyright framework has made great progress in modernizing, it is still insufficient to control the full spectrum of generative AI activities, especially when it comes to output-stage uses. As affirmed in 2025 European Parliament study, the current system of exceptions, including those under the DSM Directive, was not designed to support the expressive replication and autonomous content generation features of general-purpose AI models.[70]

2.3. Observation

Upon comparing the copyright exception in the US and the EU, it is evident that both countries have taken action to address the changing relationship between copyright and emerging technologies; however, neither framework has provided a comprehensive or proactive solution. Courts can evaluate cases individually under the U.S. fair use model, which gives it the adaptability to emerging technologies. However, this adaptability frequently leads to unpredictable outcomes. It is still unclear how far such use can go, as demonstrated by generative AI cases, particularly when AI-generated content is used in commercial settings or closely resembles original human works. The European Union, in contrast, has a rule-based framework with well-defined exceptions. Although it is a step forward, its more recent provisions, especially those that permit text and data mining, remain narrowly focused. These regulations primarily deal with the training of AI systems, but they fall short in addressing the content that these systems generate or how that content might be made profitable, for example, by using distributed ledger technologies or other digital commercialization avenues.

Therefore, it is evident that the conflict between preserving copyright holders and permitting innovation has not been entirely resolved by either system. Each model has advantages, but given the speed and scope of technological advancement, it also has apparent limitations. These findings merit serious consideration by jurisdictions such as India, where similar normative tensions are beginning to surface but have yet to be meaningfully addressed in either statute or jurisprudence.

[70] European Parliament, Policy Dept. for Just., Civ. Liberties & Institutional Affs., Generative AI and Copyright: Training, Creation, Regulation, PE 774.095, at 159–60 (2025, July).

3. Comparative overview of copyright exceptions in India, the United States, and the European Union

The preceding sections have traced the interpretation and application of copyright exceptions across three major jurisdictions. The following table emphasizes structural characteristics, technological flexibility, and the changing role of legislatures and courts in resolving copyright issues brought on by blockchain and artificial intelligence:

Country	Legal Basis	Interpretation	Judicial Engagement	Legislative Responses	Licensing Framework	Adaptability to Emerging Tech
India	Closed-list (Sec. 52, Copyright Act, 1957)	Narrow, text-bound; limited fair dealing	No rulings on GenAI, TDM, NFTs; OpenAI v. ANI pending	Digital India Act in draft; DPIIT copyright review inconclusive; no roadmap	No licensing scheme; no collective rights model	Structurally rigid; fails to address GenAI or tokenized works
USA	Open-ended (17 U.S.C. § 107 – Fair Use)	Flexible, precedent-led; tech-adaptive	Courts ruled on NFTs (Miramax, Dash); GenAI (Bartz, Kadrey, Thaler)	GenAI Disclosure Act (2024), AI Accountability Act (2025); Copyright Office guidance (2023–25)	Fragmented, voluntary market emerging; no statutory scheme	Adaptive via courts; no unified GenAI/ Digital outputs legal framework
EU	Closed-list (InfoSoc, DSM Directives)	Institutional/ national court-led	CJEU & LAION (TDM); GenAI referral pending; Juventus (NFTs)	DSM TDM exceptions; AI Act (2024); GPAI Code of Practice & Article 53(1)(d) disclosures	No structured licensing regime; provenance-focused compliance	Input-stage focused; no output-stage/NFT-specific copyright coverage

4. Results and recommendations on reforming the fair dealing regime

As the comparative analysis demonstrates, India's copyright system continues to be the least adaptable to new technologies. In contrast to the EU's closed-list model backed by specific reforms and the precedent-driven fair use doctrine in the United States, India's fair dealing regime under Section 52 of the Copyright Act, 1957, has not evolved to address generative AI or digital content generated and commercialized through new technologies. No judicial interpretation has clarified the application of copyright to AI-generated, except for on-going OpenAI v. ANI case. No specific amendments have followed despite the Ministry of Electronics and Information Technology and the Parliamentary Standing Committee on Commerce acknowledging the need for legislative reform[71]. In response to recent litigation, the Department for Promotion of Industry and

[71] Parliamentary Standing Committee on Commerce. (2021, July). Review of Intellectual Property Rights Regime in India; Meit, Y. (2021). National Strategy on Blockchain.

Internal Trade (DPIIT) has started a review process; however, there is currently no formal legislative roadmap[72].

By applying judicial mapping and comparative analysis, this study has demonstrated that India's Section 52 fair dealing framework is structurally inadequate to handle the complexity brought about by GenAI and existing framework does not even provide rights holders opt-out rights or exceptions for text and data mining (TDM), which are critical to regulate GenAI. These shortcomings are not merely theoretical; they carry substantial economic implications. According to NASSCOM, by 2035, GenAI will contribute USD 957 billion to India's GDP, or more than 15% of the country's gross value added,[73] and the adoption of AI may also result in a short-term 2.5% increase in GDP[74].

The recent constitution of an expert committee on generative AI and copyright by the Indian government provides a timely opportunity to integrate the below mentioned reforms. The following section offers targeted recommendations to reform the scope and application of fair dealing, in the light of the complex realities of generative AI and blockchain-based content creation.

4.1. Foundational reform of Section 52

The Indian government has repeatedly acknowledged its intention to modernize the Copyright Act, 1957, through official policy instruments (Parliamentary Standing Committee Report (2021), MeitY's 2024 advisory on AI governance, and the recent committee formation following the OpenAI litigation)[75]. However, this legislative intent has not resulted in actual statutory reform.

The effective modernization of India's copyright regime must commence with a foundational reform of Section 52 of the Copyright Act, 1957, particularly its provisions concerning fair dealing. As demonstrated in Section 3 of this paper, the development of fair dealing jurisprudence is limited by the strict, comprehensive structure of Section 52, not by judicial inconsistency. As seen in Oxford University Press (2008), Civic Chandran (1996), ESPN Software (2008), and Shemaroo Entertainment Ltd. (2022), the existing provision restricts judicial discretion and leads to fact-specific, profit-driven decisions, by failing to define key terms like "reporting," "instruction," and "criticism and review," and by providing no guidance on acceptable reproduction thresholds[76]. This legislative obsolescence has

72 DPIIT. (2025, Apr. 28). Constitution of Committee on AI and Copyright.

73 NASSCOM. (2024). The Economic Potential of Generative AI in India, at 6.

74 Ibid.

75 Ibid.

76 See case mapping and judicial analysis in Section 2.

led courts to decide that modern content formats such as chat shows on television do not qualify for protections due to conceptual inconsistency with the language of the statute, thereby leaving the status of AI-generated outputs similarly uncertain. As such, in order to reflect modern forms of content creation and consumption, such as text and data mining, AI training, and digital reuse, Section 52 needs to be reorganized to incorporate precisely defined, technologically relevant exceptions.

4.2. Integrating comparative lessons

Building on the necessity of defining key terms in Section 52, a comparative analysis of the European Union's statutory exception framework and the US fair use doctrine yields a second important recommendation for India's copyright reform. For interpretive guidance, Indian courts have occasionally referred to foreign jurisprudence. Courts made implicit references to the U.S. four-factor fair use test in ESPN Software (2008) and Yashraj Films v. India TV (2012), while the three-step test included in the EU's InfoSoc Directive was used in Super Cassettes v. Hamar TV Network (2010). However, as the judicial mapping clarifies, these comparative borrowings have frequently served more as rhetorical support than as substantive legal reasoning; they have been used cautiously when statutory ambiguity is allowed[77].

Despite three distinct approaches to copyright exceptions, the U.S and EU frameworks face substantial limitations when applied to generative AI and blockchain-based assets. In this paper, Section 3 "Comparative overview of copyright exceptions in India, the United States, and the European Union" demonstrates that fair use doctrine struggles to accommodate high-fidelity outputs and systemic economic disruption, while the EU's TDM exceptions and three-step test remain input-focused and lack the potential to regulate commercial AI outputs[78]. India currently lacks dedicated TDM exceptions. Section 52 of Copyright Act, 1957 fair dealing provision in India does not offer certainty for large-scale automated data analysis such as text and data mining and commercially motivated uses. However, recent developments indicate that TDM and related reforms is under consideration[79].

---

77 See judicial analysis in Section 2. (referencing ESPN Software India Pvt. Ltd., Yashraj Films Pvt. Ltd., Super Cassettes Industries Ltd., NDTV Ltd., ANI Media Pvt. Ltd., and Galatta Media Pvt. Ltd.).

78 Ibid.

79 India's Copyright Law and Artificial Intelligence: Time for a Rethink, Maheshwari & Co. (2025, Apr.). https://clck.ru/3QswPX; Balancing Innovation & Rights: A Copyright Policy Proposal for AI Training in India, IIPRD (2025, Apr.). https://clck.ru/3QswNf

To ensure Indian copyright law continues to uphold both the creator's rights and foster innovation, India must create a specific, technology-neutral exception for data and text mining. A clause must be added as a new clause under Section 52. It should specifically permit automated tools to replicate and extract copyrighted content for computational analysis, including machine learning system deployment, testing, and training. The statutory wording should also make it clear that such actions shall not be considered infringement if (a) the user has legal access to the underlying content and (b) the output produced, in any format, is not a direct reproduction of the protected expression or does not violate other specific copyright limitations.

In India, a model that is input-only and narrowly drafted, like the EU DSM Directive, would be ineffective, as Lucchi (2025) points out in his analysis for the European Parliament. The European Union's TDM framework has proven structurally incapable to control generative outputs that imitate style or turn datasets into expressive content[80]. Unlike Article 4 of DSM, which is incompatible with decentralized technologies[81], India's TDM exception should to be forward-thinking and output-conscious. It must offer legal certainty for data ingestion and use in AI system development, as well as for the legitimate distribution of AI system outputs, in other commercial digital forms.

Instead of frequently relying on the fair use principle developed under U.S copyright law, India should pursue a statutory approach that emphasizes legislative clarity without sacrificing technological flexibility. As seen in Section 2.1 "Fair use in the United States", the open-ended nature of fair use has proven flexible but structurally inadequate when applied to generative technologies that operate through large scale ingestion[82]. As such, India should adopt a purpose-based statutory exception that expressly permits the use and reproduction of copyrighted works for computational applications, including information analysis, model evaluation, and machine learning, as long as (a) the use is not meant for the primary consumption or enjoyment of the content itself, and (b) the outputs do not amount to direct reproduction of protected expression. As long as the user has legal access, such a model can allow legitimate TDM for all subjects and for all uses, including commercial and legitimate digital use. This approach reduces the reliance on case-by-case judicial balancing and minimizes interpretive uncertainty.

---

80 European Parliament, supra note 12 6 at 22–25.

81 Chauhan, K. (2025).Text and Data Mining Under Indian Copyright Law: Need for Reform. J. Intell. Prop. Rts., 30(1), 8–9.

82 See 2.1 Fair use In U.S

4.3. Enhancing legal accountability in generative AI through training data disclosure

India's exisitng regulatory approach to artificial intelligence (AI) remains largely concerned with controlling the results of AI systems, especially with regard to the distribution and labeling of AI-generated content. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which impose due diligence obligations on online platforms to moderate harmful or misleading outputs, and the 2024 MeitY Advisory on Responsible AI, which requires the labeling of synthetic content, are recent policy instruments that reflect this approach[83]. While these measures address issues such as misinformation, electoral interference, and reputation harm, they do not meaningfully regulate the input-side of AI, particularly the use of copyrighted or sensitive data during model training. Recent policy documents, including the Press Information Bureau's 2023 National Strategy for Artificial Intelligence and the 2024 MeitY Advisory, highlight the importance of accountability, transparency, and equity. However, they fail to consider the ethical and legal ramifications of data collection methods used during the model-training phase[84].

While copyright exceptions in the EU and U.S. face challenges in addressing generative AI, legislative frameworks, especially in European Union, have started to take a more direct approach to the creation and training of AI models. India's approach to AI regulation needs to evolve beyond existing limitations. India must adopt mandatory disclosures for AI developers, particularly with regard to the generative model training datasets. These requirements needs to be similar to the EU AI Act's Article 53(1)(d), which requires developers of general-purpose AI (GPAI) to publish structured summaries of the sources of their training data,[85] and U.S. proposals such as the Generative AI Copyright Disclosure Act (2024), which aims for similar transparency regarding copyrighted works[86]. Given

---

83 Ministry of Electronics and Information Technology (MeitY), Advisory for Responsible Use of Artificial Intelligence, 2024 [hereinafter MeitY Advisory]; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021), amended by G.S.R. 228(E) (2023, Apr. 6).

84 Press Information Bureau. National Strategy for Artificial Intelligence, 2023.

85 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), art. 53(1)(d), 2024 O.J. (L 1689) 1; see also Explanatory Notice and Template for the Public Summary of Training Content for GPAI Models, European Commission, C(2025) 5235 (approved 24 July 2025), described by commentators as introducing mandatory template-based data summaries under Article 53(1)(d).

86 Accountability and Personal Data Protection Act, S. 2367, 119th Cong. § 3 (2025) (introduced July 21, 2025).

the limitations in the Information Technology Act, 2000, such disclosure rules could be introduced as part of a future omnibus Digital India Act[87].

The General-Purpose AI Code of Practice in EU, which is not legally binding, provides a useful model for best practices in sourcing datasets, stopping illegal copying, setting up complaint procedures, and guaranteeing accountability[88]. MeitY and the Department for Promotion of Industry and Internal Trade (DPIIT) could work together to create a comparable Code adapted to India's particular legal and technological environment and imposing auditability requirements for developers utilizing sizable datasets that contain user-generated or copyrighted content, much like the record-keeping requirements outlined in Articles 10 and 53 of the EU AI Act[89].

4.4. Remuneration based model

In addition to controlling AI outputs and enhancing training data transparency, a forward-thinking licensing framework is necessary to ensure that authors receive fair compensation for their creations when they are incorporated into generative AI systems. However, the absence of a functional licensing market for AI training data in India poses a structural barrier for equitable remuneration[90]. MEP Axel Voss's 2025 draft report on Copyright and Generative AI, which suggests a temporary compensation mechanism whereby general-purpose AI (GPAI) developers pay a 5–7% levy on their global revenues, is the first step in this direction taken by the European Union[91]. By providing rights holders with instant compensation without presenting it as a "global license," this model aims to address the absence of a licensing market. India could adopt this model by instituting a statutory compensation plan for major AI developers, with licensing and distribution management handled by the Copyright

87 Phillips, P., & Avasarala, S. (2023, Mar. 27). Digital India Act: Evolving Clarity & Challenges (Lakshmikumaran & Sridharan Attorneys). (discussing how the Digital India Act has been proposed to overhaul the IT Act and establish a standardized, future-proof digital governance regime).

88 European Commission. (2025, July 10). General-Purpose AI Code of Practice. covering transparency, copyright, and safety obligations for providers of general-purpose AI models under the EU AI Act; see also EU Code of Practice helps industry comply with AI Act rules on general-purpose AI models, press release (2025, July 11).

89 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 March 2024 Laying Down Harmonised Rules on Artificial Intelligence (AI Act), arts. 10, 53, 2024 O.J. (L 230) 1 (EU) (on data governance and transparency obligations for general-purpose AI models).

90 IIPRD, Balancing Innovation & Rights: A Copyright Policy Proposal for AI Training in India (2024, Sept. 4). (noting that "individual licensing for AI training data is impractical"). https://clck.ru/3Qsy58

91 European Parliament. (2025, 10 July). Draft Report on Copyright and Generative AI, Rapporteur Axel Voss, Committee on Legal Affairs (JURI), at 5–7.

Office or another designated organization. Similar to Article 53(1)(d) of the EU AI Act, a rebuttable presumption that copyright-protected works have been used in training could improve legal enforceability unless developers provide structured disclosures of their data sources. This would encourage transparency and lessen the evidentiary burden on creators.

4.5. Blockchain technology for accountability and licensing in generative AI

To ensure accountability, fair remuneration, and enforceability of the suggested reforms establishing a technology infrastructure that can facilitate transparent licensing, data provenance, and automated rights management is equally important. Blockchain technology has the potential to address the same, by creating unchangeable records of training inputs, licensing terms, and output provenance; it can improve accountability, transparency, and compensation throughout the generative AI life cycle. Smart contracts can automate licensing and compensation through a blockchain-based registry of training datasets, guaranteeing that authors receive payment when their creations are utilized to build models or produce derivative outputs. For example, copyright metadata can be embedded in hashed dataset logs and verifiable blockchain-based licenses, allowing developers to reveal inputs and initiating automatic payments upon commercialization of outputs[92]. This approach aligns with proposal in EU, where blockchain is being investigated for provenance tracking, licensing under the AI Act, and copyright modernization initiatives[93]. It directly addresses the limitations of conventional copyright enforcement, which remains ineffective and retroactive in digital settings where large-scale training of generative AI models occurs without sufficient transparency or licensing frameworks. To enforce dataset disclosures, monitor model usage, and implement statutory compensation schemes in India, the Copyright Office or MeitY could combine blockchain-backed systems with the proposed Digital India Act. This would ensure compliance through clear, tamper proof audit trails[94].

---

92 Lai, T., & De Filippi, P. (2025, Jan. 31). A Collaborative Effort to Design and Promote Blockchain-Based IP Tools and Standards for Rightful Generative AI, Medium.

93 European Parliament. (2025, July). Generative AI and Copyright: Training, Creation, Regulation, Policy Dept. for Legal Affairs, PE 774.095, at 22–26.

94 Mishra, T. (2025, June 3). Reversing the Opt-Out Burden: Why AI Firms Should Bear Licensing Obligations for Training Data, SpicyIP. https://spicyip.com

Conclusions

The analysis showed that generative AI and blockchain-based creative systems expose deep structural gaps in existing copyright frameworks, especially in India. While courts in multiple jurisdictions are already struggling with cases like Getty Images v. Stability AI, Bartz v. Anthropic, and ANI v. OpenAI, India's closed-list fair dealing model and the architecture of Section 52 of the 1957 Act leave judges with even fewer doctrinal tools than their counterparts in the United States or European Union. A comparison with the U.S. fair use doctrine and the EU's text and data mining exceptions demonstrates that Indian law is currently ill equipped to deal with either the training phase of GenAI systems or the attribution and exploitation of their outputs. Against this backdrop, the paper's proposals (introducing tailored TDM exceptions, optout mechanisms, statutory licensing for training datasets, and blockchain-based accountability) are not merely desirable but necessary preconditions for a workable GenAI copyright settlement in India. These reforms align with, and should inform, the work of the expert committee on generative AI and copyright established by the Indian government in 2025, offering a concrete legislative roadmap for reconciling technological innovation with the protection of creative labor.

References

Al-Busaidi, A. S. (2024). Investigating the impact of generative artificial intelligence on copyright law: A comparative analysis. *Computer Law & Security Review*, *54*, 105928. https://doi.org/10.1016/j.clsr.2024.105928sciencedirect

Balganesh, S. (2013). *The constitutionalization of fair use*. Oxford University Press.

Balganesh, S. (2017). Fair use and fair dealing: Two approaches to limitations and exceptions in copyright law. In I. A. Calboli, & G. F. Dinwoodie (Eds.), *The Cambridge handbook of international and comparative copyright law* (pp. 286–305). Cambridge University Press.

Bonadio, E., & McDonagh, L. (2025). Modernising EU copyright in the generative AI era: Text and data mining, transparency, and authors' rights. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5523838

Buick, A. (2025). Copyright and AI training data—Transparency to the rescue? *Journal of Intellectual Property Law & Practice*, *20*(3), 182–192. https://doi.org/10.1093/jiplp/jpae102

Chauhan, K. (2025). Artificial intelligence and copyright in India. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5096997

Chopra, P. (2025). Generative AI, copyright and personality rights. *Library and Information Discourse Analysis*, *16*(2), 243–266. https://doi.org/10.17323/2658-3253.2025.16.2.243-266

Dornis, T. W. (2025). Generative AI training and copyright law: Fair use, fair dealing, and the EU's new regime. *arXiv*. https://arxiv.org/pdf/2502.15858.pdfarxiv

Grodzinsky, F. S., Tavani, H. T., & Wolf, M. J. (2007). Private use as fair use: Is it fair? *ACM SIGCAS Computers and Society*, *37*(3), 8–13. https://doi.org/10.1145/1327325.1327326acm

Hauck, R. (2021). Blockchain, smart contracts and intellectual property: Using distributed ledger technology to protect, license and enforce intellectual property rights. *Legal Issues in the Digital Age*, *1*(1), 17–41. https://doi.org/10.17323/2713-2749.2021.1.17.41lida.hse

Li, K. (2024). Copyright protection during the training stage of generative AI: A comparative study of US and EU law. *Computer Law & Security Review*, *54*, 105983. https://doi.org/10.1016/j.clsr.2024.105983sciencedirect

Li, Y., & Wang, S. (2024). A copyright-aware blockchain framework for digital content licensing. *Computers & Security*, *134*, 103539. https://doi.org/10.1016/j.cose.2024.103539sciencedirect

Lund, D. S., & Samuelson, P. (2024). Tiered copyrightability for generative artificial intelligence. *AI and Ethics*, *4*(2), 201–220. https://doi.org/10.1002/aaai.70018onlinelibrary.wiley

Mohammed, A. F. (2025). Fair dealing or unfair system? Copyright enforcement, Content ID, and user rights in India's platform economy. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5367971papers.ssrn

Rosati, E. (2025a). Copyright exceptions and fair use defences for AI training: EU, US and beyond. *European Journal of Risk Regulation*, *16*(3), 421–446. https://doi.org/10.1017/err.2025.15cambridge

Rosati, E. (2025b). The development of generative AI from a copyright perspective: EU text and data mining, opt-outs, and fundamental rights. *European Parliamentary Research Service Study*. https://doi.org/10.2861/GENAI.2025europarl.europa

Sood, P. (2024). Fair dealing in India: An analysis vis-à-vis fair use in the United States. *Journal of Intellectual Property Rights*, *28*, 560–568. https://doi.org/10.56042/jipr.v29i6.7528niscpr

Volkova, K. Y. (2021). Comparison of fair use and fair dealing concepts in copyright law. *Scientific and Technical Libraries*, *6*, 57–69. https://doi.org/10.33186/1027-3689-2021-6-57-69ntb.gpntb

Xie, R., Zhang, J., & Liu, H. (2024). A digital resource copyright protection scheme based on blockchain cross-chain technology. *Heliyon*, *10*(5), e228617. https://doi.org/10.1016/j.heliyon.2024.e228617sciencedirect

Yu, F., Li, Z., & Wang, J. (2023). A copyright-preserving and fair image trading scheme based on blockchain. *IEEE Transactions on Industrial Informatics*, *19*(7), 9321–9332.

Appendix

Chronological mapping of Indian fair dealing cases (1959–2025)

No.	Case Name & Citation	Year	Key Legal Issue(s)	Judicial Interpretation of Fair Dealing	Critical Observation	Relevance to Emerging Technologies
1	Blackwood and Sons Ltd. v. A.N. Parasuraman	1959	Unauthorized reproduction of textbooks for educational use	Educational purpose acknowledged, but fair dealing narrowly applied; no foreign comparative references adopted	Early judicial restraint; protection of commercial interests even in academic use; no willingness to evolve fair dealing via international influence	Offers little flexibility for AI/ML or TDM exceptions in academic or non-commercial contexts
2	Shyam Lal Paharia v. Gaya Prasad Gupta, AIR 1971 All 192	1970	Copying of a compilation with partially original and partially copied content	Recognized infringement even though some portions were original; protection seemed to hinge on labor and effort	Reflects "sweat of brow" approach; effort-based originality doctrine dominant; lacks modern creative threshold	Reliance on effort over creativity misaligns with AI outputs where reproduction is not tied to human labor
3	V. Ramaiah v. K. Lakshmaiah	1988	Use of textbook content in a guidebook	Emphasized educational use and proportionality; accepted fair dealing as defense	Set precedent for proportionality, but gave vague guidance on what counts as "independent contribution"	No clarity on threshold for transformative use or independent input, relevant for generative remixing or summarization tools
4	Civic Chandran v.Ammini Amma, AIR 1996 Ker 291	1996	Use of prior drama in a counter-drama with criticism	Court adopted activist approach; invoked transformative purpose and fairness; avoided rigid quantitative tests	Progressive turn; relied on UK judgment (Hubbard v. Vosper); qualitative fairness; restraint in not setting rigid rules	Closest early adoption of transformative use; yet lack of codification makes it fragile for AI/deep remix culture
5	Eastern Book Co. v. D.B. Modak, (2008) 1 SCC 1	2008	Originality of headnotes and editorial contributions	Adopted "minimal creativity" standard; used Canadian and UK precedents; cautious fair dealing	Shows willingness to adopt global doctrine, but limited support in Indian law; weak transformative framework	Inconsistent guidance for algorithmic summaries, annotations, or AI-edited material
6	Oxford Univ. Press v. Narendra Publishing House	2008	Reproduction of educational content in guides	Liberal interpretation of fair dealing; invoked U.S. transformative use; ignored market harm	Progressive, but structurally weak due to absence of statutory transformative test; dismissive of economic impact	Courts inclined toward AI-enabling logic, but lack clarity on how much transformation suffices
7	ESPN Software India v. T.V. Today Network	2008	Use of sports footage in news	Applied four-factor fair use test implicitly; rejected fixed time benchmarks; prioritized market harm	Acknowledges foreign doctrines; courts rely on context-specific factors; inconsistencies remain	Highlights risk of judicial borrowing without harmonization; key for AI video summarizers, remixers

8	Cambridge Univ. Press v. B.D. Bhandari	2009	Use of grammar exercises and model answers in student books	Held use fell under fair dealing; invoked transformative use; no standard defined for "extent"	Permits extensive copying without clarity; undermines predictability in education-related AI training	Ambiguity can complicate AI datasets that rely on textbook or exam-content reuse
9	Super Cassettes v. Hamar TV Network	2010	Use of songs in news/reporting programs	Rejected transformative use; followed Berne/ TRIPS 3-step test; stressed substantiality	Rigid interpretation; restrained from recognizing evolving uses; conservative benchmark	Not friendly to AI-driven quotation, commentary, or hybrid content creation
10	India TV v. Yashraj Films, FAO(OS) 583/2011	2012	Use of clips in talk shows and ads; claimed de minimis	Denied fair use under S.52; accepted de minimis without expanding S.52; applied U.S. four-factor test	Judicial restraint; emphasized Parliament's role in reform; relied on quantitative de minimis	Sign of judiciary limiting its scope; highlights structural inflexibility for emerging tech, especially AI/media overlaps
11	ICC Development (International) Ltd. v. NDTV	2012	Unauthorized use of sports footage in reporting	Prioritized broadcaster's commercial rights over evolving fair use norms; declined to apply flexible foreign interpretations	Confirms judicial preference for literal statutory reading over public interest or tech evolution	Undermines AI access to public interest content in commercial broadcast archives
12	Chancellor v. Rameshwari Photocopy Services	2016	Fair use for educational copying (Trial & Division Bench)	Court refused to impose quantitative limits; emphasized parliamentary intent; cautious approach to fair dealing	Affirmed broader educational access; restrained from legislating; lacked detailed economic analysis	Crucial precedent supporting AI/ML training on academic corpora; judicial caution means future scope still uncertain
13	Ravinder Singh v. Evergreen Publications	2018	Use of question papers in guidebooks	Rejected transformative claims; emphasized substitution and market competition	Restrictive and commercially protective; no innovation space for adaptive educational AI	Reduces scope for training models using test-prep or academic simulation data
14	Super Cassettes v. Shreya Broadcasting	2019	Use of song in TV satire/criticism	Followed Hamar; refused to analyze transformation; focused on literal criticism	Avoided market analysis or editorial transformation; narrow interpretive method	Not suitable for evolving formats like AI parody, review, satire, or auto-generated mashups
15	Tips Industries v. Wynk Music	2019 / 2022	Applicability of S.31-D to streaming platforms	Declared streaming non-broadcast; fair dealing inapplicable to on-demand use	Refused to adapt S.52 to digital consumption; deferred to Parliament	Restrictive for generative music AI; reinforces analog-specific interpretations
16	Shemaroo Ent. Ltd. v. News Nation Network	2022	Post-license revocation use of copyrighted clips	Emphasized license history over nature of use; burden on defendant at interim stage	Contractual history prioritized over fair dealing logic; ignored editorial justification	Burdens AI-driven broadcasters relying on secondary content reuse or commentary

17	St+Art Indian Foundation v. Acko Gen. Insurance	2023	Use of celebrity photos in ad campaigns	Required proof at interim stage; deferred trial for S.52; rejected foreign fair use analogies	Strong formalism; limits experimental or editorial reuse unless clear from start	Problematic for AI-generated collages, memes, or image-based editorial uses
18	Galatta Media (P) Ltd. v. Nian Media (P) Ltd., 2024 SCC OnLine Mad 5682	2024	Use of film clips and celebrity commentary in online shows	Court declined to apply foreign transformative use standards; placed early evidentiary burden on defendant	Judicial restraint; refused to expand S.52 despite digital format and foreign precedents; reversed burden at interim stage	Illustrates limits of fair dealing for AI-generated commentary, celebrity content remix, and social video platforms
19	ANI Media Pvt. Ltd. v. Mohak Mangal	2025	Use of news footage in critical explained content	At interim stage; fair dealing argued as transformative; court showed doctrinal tension	Highlights structural struggle in applying narrow statutory fair dealing to dynamic digital expression	Test case for whether Indian courts can stretch S.52 to fit YouTube* explainers, AI-driven news summaries

* The foreign person owning the YouTube informational resource violates the legislation of the Russian Federation.

Author information

K. S. Amith Sriram – Assistant Professor, Ramaiah College of Law
Address: Multipurpose Block, Gate No. 8 или 10, MSR Nagar, 560054 Bengaluru, India
E-mail: amithsriram.007@gmail.com
ORCID ID: https://orcid.org/0009-0005-7023-3920

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – August 13, 2025
Date of approval – August 26, 2025
Date of acceptance – December 20, 2025
Date of online placement – December 25, 2025

Научная статья
УДК 34:004:346.6:004.8:347.78
EDN: https://elibrary.ru/xeltpk
DOI: https://doi.org/10.21202/jdtl.2025.24

Авторское право перед вызовами генеративного искусственного интеллекта: судебная практика и законодательные стратегии в Индии, США и Европейском союзе

К. С. Амит Шрирам

Юридический колледж Рамайя, Бангалор, Индия

Ключевые слова

авторское право,
анализ данных,
блокчейн,
генеративный искусственный интеллект,
искусственный интеллект,
право,
правовое регулирование,
сравнительное правоведение,
судебная практика,
цифровые технологии

Аннотация

Цель: проведение сравнительного анализа судебной интерпретации доктрин добросовестного ведения сделок и добросовестного использования в системах авторского права Индии, Соединенных Штатов и Европейского союза в контексте вызовов, порождаемых развитием генеративного искусственного интеллекта и технологий блокчейна.

Методы: в работе использован комплекс научных методов, включающий сравнительно-правовой анализ законодательства трех юрисдикций, систематический анализ судебной практики Индии, догматический метод толкования нормативных актов, а также структурно-функциональный подход к исследованию правовых институтов. Особое внимание уделено изучению индийской судебной практики применения доктрины добросовестного ведения сделок за более чем 60 лет, анализу американской доктрины добросовестного использования с ее четырехфакторным критерием и исследованию европейской системы законодательных исключений для интеллектуального анализа текстов и данных. Методологическая основа исследования включает историко-правовой метод для выявления эволюционных тенденций судебного толкования исключений из авторского права, формально-юридический метод для анализа нормативного содержания правовых институтов, а также метод правового моделирования для разработки рекомендаций по совершенствованию законодательства в области регулирования генеративного искусственного интеллекта и блокчейн-технологий.

Результаты: проведенное исследование убедительно демонстрирует структурное несоответствие индийской системы исключений из авторского права по принципу закрытых списков для регулирования генеративного искусственного интеллекта и блокчейн-технологий.

Установлено, что индийская доктрина добросовестного ведения сделок характеризуется пятью фундаментальными ограничениями: чрезмерной привязанностью к буквальному толкованию законодательного текста, отсутствием концепции трансформирующего использования, неспособностью адаптироваться к цифровым форматам, правовым пробелом в регулировании результатов работы искусственного интеллекта и существенно ограниченным применением. Сравнительный анализ выявил, что американская система достигает структурных пределов при регулировании масштабного использования данных, тогда как европейская модель ограничивается этапом ввода данных и не охватывает коммерциализацию результатов работы искусственного интеллекта.

Научная новизна: впервые проведен комплексный сравнительно-правовой анализ применения доктрин добросовестного ведения сделок и добросовестного использования к генеративному искусственному интеллекту и блокчейн-технологиям на основе систематизации более чем шестидесятилетней судебной практики трех правовых систем, позволивший выявить структурные ограничения как открытых, так и закрытых моделей исключений из авторского права и обосновать необходимость перехода к комплексному регулированию полного жизненного цикла создания и коммерциализации контента, генерируемого искусственным интеллектом.

Практическая значимость: результаты исследования могут быть использованы при разработке национальных стратегий регулирования искусственного интеллекта, реформировании системы исключений из авторского права, внедрении технологически нейтральных норм для интеллектуального анализа данных, создании механизмов раскрытия информации об обучающих наборах данных и реестров отказа правообладателей, а также при модернизации системы коллективного управления правами с применением инструментов блокчейна.

Для цитирования

Амит Шрирам, К. С. (2025). Авторское право перед вызовами генеративного искусственного интеллекта: судебная практика и законодательные стратегии в Индии, США и Европейском союзе. *Journal of Digital Technologies and Law*, *3*(4), 598–635. https://doi.org/10.21202/jdtl.2025.24

Список литературы

Al-Busaidi, A. S. (2024). Investigating the impact of generative artificial intelligence on copyright law: A comparative analysis. *Computer Law & Security Review*, *54*, 105928. https://doi.org/10.1016/j.clsr.2024.105928sciencedirect

Balganesh, S. (2013). *The constitutionalization of fair use*. Oxford University Press.

Balganesh, S. (2017). Fair use and fair dealing: Two approaches to limitations and exceptions in copyright law. In I. A. Calboli, & G. F. Dinwoodie (Eds.), *The Cambridge handbook of international and comparative copyright law* (pp. 286–305). Cambridge University Press.

Bonadio, E., & McDonagh, L. (2025). Modernising EU copyright in the generative AI era: Text and data mining, transparency, and authors' rights. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5523838

Buick, A. (2025). Copyright and AI training data—Transparency to the rescue? *Journal of Intellectual Property Law & Practice*, *20*(3), 182–192. https://doi.org/10.1093/jiplp/jpae102

Chauhan, K. (2025). Artificial intelligence and copyright in India. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5096997

Chopra, P. (2025). Generative AI, copyright and personality rights. *Library and Information Discourse Analysis*, *16*(2), 243–266. https://doi.org/10.17323/2658-3253.2025.16.2.243-266

Dornis, T. W. (2025). Generative AI training and copyright law: Fair use, fair dealing, and the EU's new regime. *arXiv*. https://arxiv.org/pdf/2502.15858.pdfarxiv

Grodzinsky, F. S., Tavani, H. T., & Wolf, M. J. (2007). Private use as fair use: Is it fair? *ACM SIGCAS Computers and Society*, *37*(3), 8–13. https://doi.org/10.1145/1327325.1327326acm

Hauck, R. (2021). Blockchain, smart contracts and intellectual property: Using distributed ledger technology to protect, license and enforce intellectual property rights. *Legal Issues in the Digital Age*, *1*(1), 17–41. https://doi.org/10.17323/2713-2749.2021.1.17.41lida.hse

Li, K. (2024). Copyright protection during the training stage of generative AI: A comparative study of US and EU law. *Computer Law & Security Review*, *54*, 105983. https://doi.org/10.1016/j.clsr.2024.105983sciencedirect

Li, Y., & Wang, S. (2024). A copyright-aware blockchain framework for digital content licensing. *Computers & Security*, *134*, 103539. https://doi.org/10.1016/j.cose.2024.103539sciencedirect

Lund, D. S., & Samuelson, P. (2024). Tiered copyrightability for generative artificial intelligence. *AI and Ethics*, *4*(2), 201–220. https://doi.org/10.1002/aaai.70018onlinelibrary.wiley

Mohammed, A. F. (2025). Fair dealing or unfair system? Copyright enforcement, Content ID, and user rights in India's platform economy. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5367971papers.ssrn

Rosati, E. (2025a). Copyright exceptions and fair use defences for AI training: EU, US and beyond. *European Journal of Risk Regulation*, *16*(3), 421–446. https://doi.org/10.1017/err.2025.15cambridge

Rosati, E. (2025b). The development of generative AI from a copyright perspective: EU text and data mining, opt-outs, and fundamental rights. *European Parliamentary Research Service Study*. https://doi.org/10.2861/GENAI.2025europarl.europa

Sood, P. (2024). Fair dealing in India: An analysis vis-à-vis fair use in the United States. *Journal of Intellectual Property Rights*, *28*, 560–568. https://doi.org/10.56042/jipr.v29i6.7528niscpr

Volkova, K. Y. (2021). Comparison of fair use and fair dealing concepts in copyright law. *Scientific and Technical Libraries*, *6*, 57–69. https://doi.org/10.33186/1027-3689-2021-6-57-69ntb.gpntb

Xie, R., Zhang, J., & Liu, H. (2024). A digital resource copyright protection scheme based on blockchain cross-chain technology. *Heliyon*, *10*(5), e228617. https://doi.org/10.1016/j.heliyon.2024.e228617sciencedirect

Yu, F., Li, Z., & Wang, J. (2023). A copyright-preserving and fair image trading scheme based on blockchain. *IEEE Transactions on Industrial Informatics*, *19*(7), 9321–9332.

Сведения об авторе

Амит Шрирам К. С. – ассистент преподавателя, Юридический колледж Рамайя
Адрес: 560054, Индия, г. Бангалор, МСР Нагар, въезд 8–10
E-mail: amithsriram.007@gmail.com
ORCID ID: https://orcid.org/0009-0005-7023-3920

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.31 / Право на информацию
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 13 августа 2025 г.
Дата одобрения после рецензирования – 26 августа 2025 г.
Дата принятия к опубликованию – 20 декабря 2025 г.
Дата онлайн-размещения – 25 декабря 2025 г.

Research article
UDC 34:004:343.14:343.98.062:343.98.063
EDN: https://elibrary.ru/qjhwgw
DOI: https://doi.org/10.21202/jdtl.2025.25

Place of Digital Phonograms, Videograms, and Videophonograms in the System of Electronic Evidences: Theoretical and Methodological Principles of Classification

German N. Zubov
Independent researcher, Saint Petersburg, Russia

Keywords

digital forensics,
digital technology,
electronic evidence,
evidence,
expertise,
law,
legal proceedings,
phonogram,
videogram,
videophonogram

Abstract

Objective: to determine the place of digital phonograms, videograms and videophonograms in the system of electronic evidence in Russian judicial proceedings, to form a unified conceptual framework and classification system to ensure effective use in procedural practice.

Methods: the research is based on the universal dialectical method of cognition, general scientific methods (description, comparison, generalization, modeling, analysis, synthesis), and specific scientific methods. Special attention was paid to the system-structural analysis of regulatory legal acts, state standards in the field of information technology, and international documents regulating work with digital evidence. The author applied methods of criminalistic research, a formal legal method of interpreting procedural norms, and a comparative analysis of foreign experience in regulating electronic evidence.

Results: the study identified and systematized the key reasons for the legal uncertainty of electronic evidence: a variety of representation forms, high data vulnerability, insufficient competence of the proving subjects, and inconsistency with traditional methods of evidence recording. The author developed an original classification of electronic evidence and digital phonograms, videograms, and videophonograms, using criteria such as the form of data presentation, recording method, and nature of information media. Universal definitions of the basic concepts are formulated: electronic evidence, digital evidence, digital phonogram,

videophonogram, data carriers, a copy of digital evidence. The necessity is substantiated to harmonize procedural norms based on state standards of information technologies and international experience.

Scientific novelty: for the first time, a comprehensive methodology was developed to form the conceptual apparatus and classification of electronic evidence, integrating state standards on information technology with criminalistic and procedural aspects of evidence recording. Universal terms and definitions were introduced, which had been absent in the current Russian legislation. They were adapted for all types of legal proceedings, taking into account the specifics of the digital environment. A typical model of working with digital evidence was proposed, with identification, collection, receipt, preservation, analysis and presentation stages. The category of digital phonograms, videograms and videophonograms was proved to be a subtype of electronic discrete digital evidence.

Practical significance: the results can be used to improve procedural legislation regarding the regulation of work with electronic evidence. They can help to develop departmental instructions and practical recommendations for investigators, specialists and experts on the identification, collection, fixation, verification and evaluation of digital evidence. The proposed classification and conceptual framework contribute to the unification of approaches to the procedural design of electronic evidence. The result is minimizing procedural errors, increasing the competence of the proving subjects, and ensuring the admissibility and reliability of digital phonograms, videograms and videophonograms. The research materials are applicable in the training of lawyers, investigators, and forensic experts specializing in digital forensics

For citation

Zubov, G. N. (2025). Place of Digital Phonograms, Videograms, and Videophonograms in the System of Electronic Evidences: Theoretical and Methodological Principles of Classification. *Journal of Digital Technologies and Law, 3*(4), 636–659. https://doi.org/10.21202/jdtl.2025.25

Contents

Introduction

Russian legislation allows the use of phonograms, videograms and videophonograms (further referred to as PhVVph)[1] as evidence in administrative, arbitration, criminal and civil proceedings, regardless of the form – analog or digital, and the method of their presentation – a file in the memory of a video recording device, publication on a social network, etc.

Such evidence may include PhVVph recorded:

– as part of operational investigative activities;

– by an investigator or an expert during conducting investigative actions and taking minutes of court sessions;

– by other participants in the process (an accused, a victim, a witness, a plaintiff, a defendant, etc.);

– by various general-purpose automated systems for collecting and processing audio and visual information: video surveillance, telephone recordings, etc.

However, even a cursory review of the texts of procedural laws indicates a lack of uniformity, even in naming objects containing evidentiary audiovisual information.

For example, the result of recording audio information on a tangible medium (further referred to as a phonogram) is called:

– audio recording (Russian Administrative Procedural Code, Russian Civil Code, Russian Criminal Procedural Code);

– audio materials (Russian Code of Administrative Offenses);

– audio recording materials (Russian Criminal Procedural Code);

– sound recording materials (Russian Code of Administrative Offenses);

– phonogram (OIA law[2], Russian Civil Code, Russian Code of Administrative Offenses).

The result of recording visual or audiovisual information (further referred to as a videogram or a videophonogram, respectively) is referred to as:

– videogram (OIA law);

– video recording (Russian Administrative Procedural Code, Russian Criminal Procedural Code);

– video materials (Russian Code of Administrative Offences);

– the materials of the video recording (Russian Code of Administrative Offences).

Procedural laws do not distinguish between a videogram and a videophonogram, or between digital or analog PhVVphs, although these differences objectively exist and may affect the processing of audio-visual information with evidentiary value, as well as its verification and evaluation as evidence. Consider the following example. An investigator

---

1 According to the wording of GOST 13699-91 “Recording and reproduction of information. Terms and definitions”. https://clck.ru/3QH6Ac

2 Here and further – Federal law “On investigative activity” of 12.08.1995 No. 144-FZ (OIA law).

asked an expert if there were traces of editing on a "video recording" and submitted the videophonogram for examination. The expert, in accordance with the "letter" of the question, studied the video in the videophonogram, but ignored the sound, which, according to the case file, contained evidentiary information and was edited (Zubov, Timoshenko, 2014).

This is not surprising, given that regulatory legal acts – both laws and departmental instructions, guides, recommendations, etc. – lack even the basic concepts of PhVVphs such as the concepts of electronic and digital evidence. In the procedural laws and resolutions of the higher courts, these concepts are customarily equaled to information presented "in electronic form" (Russian Code of Administrative Offenses); on "electronic media" (Russian Criminal Procedural Code); or "electronic documents" (Russian Criminal Procedural Code and Russian Administrative Procedural Code). At the same time, there is also no explicit definition of the term "electronic media" in the texts of regulatory legal acts. Its meaning is revealed through context and indirect indications. As a rule, "electronic media" is understood as a device for recording, storage and use of digital data exclusively.

The Law "On information, information technologies and information protection"[3] gives the following definition of an "electronic document": "documented information presented in electronic form, that is, in a form suitable for human perception using electronic computers, as well as for transmission over information and telecommunication networks or for processing in information systems". It is not applicable to digital PhVVphs, since digital PhVVphs, the electronic origin of which is beyond doubt, can be recorded or reproduced without using a computer. It is equally important that, while the Russian Criminal Procedural Code classifies PhVVphs as "other documents", other procedural laws classify documents as written evidence, to which PhVVphs clearly do not belong.

A more precise definition of an "electronic document" is contained in the Law "On arbitration (arbitration proceedings) in the Russian Federation"[4]: "an electronic document transmitted through communication channels – information prepared, sent, received or stored using electronic, magnetic, optical or similar means, including electronic data exchange and e-mail".

Thus, one can state that Russian legislation lacks a single, universal, exhaustive legal definition of "electronic evidence" (further referred to as EE) and does not reflect the generic features and classification of EE. This prevents an understanding of the specific features of using this type of evidence in court proceedings and their objective assessment in terms of admissibility and reliability. It also hinders creating practical guides for investigators and experts working with this type of evidence.

---

3 On information, information technologies and information protection. No. 149-FZ of 27.07.2006. (2006). KonsultantPlyus. https://clck.ru/3QH6Dq

4 On arbitration (arbitration proceedings) in the Russian Federation. No. 382- FZ of 29.12.2015 (ed. of 08.08.2024). KonsultantPlyus. https://clck.ru/3QH6YV

A similar situation is observed in the publications of Russian practicing lawyers and legal scholars (Voronin, 2021; Malyk, 2023; Politsian, 2022; Cheretskikh, 2023), who also cannot come to a consensus on EE. Some do not see the difference between digital and electronic evidence, others classify them as different types, but both note the imperfection of Russian legislation regarding the use of EE and, as a rule, speak of the need to view EE as a separate type.

1. Causes of legal uncertainty of electronic evidences

There are several key factors causing the legal uncertainty of EE.

First and foremost, there is the variety of EE forms and types that do not correspond to the written form of recording evidentiary information accepted in procedural practice.

The evidences, which is currently commonly referred to as electronic, include: electronic documents per se, including electronic images of written documents; correspondence in e-mail applications and messengers; files of various formats; databases, metadata; server logs, etc. Some of them can be represented: in physical form (on a tangible medium, for example, in the external memory of a sound or video recording device); in virtual form (for example, a videophonogram in the YouTube[5] Internet service). At the same time, evidentiary information can be relatively easily, often deceptively easily, transferred from one medium to another and exist in many indistinguishable copies; its reproduction and perception in some cases are impossible without the use of software and hardware, the use of which often requires the user to have special knowledge in the field of information technologies.

All this undoubtedly complicates the identification, collection, receipt, classification and description of EE in the protocol, as well as the unification of approaches to their assessment. It also necessitates the use of various verification technologies, including those unknown for the participants in the process: electronic signatures (Russian Administrative Procedural Code, Russian Civil Code, Russian Code of Administrative Offences, Russian Criminal Procedural Code, Law on electronic signature[6]); hash functions (GOST R ISO/IEC 27037[7], GOST R 57429[8]); a unique set of technical characteristics and metadata of PhVVphs; UUID[9].

---

5 The foreign person owning the YouTube informational resource violates the legislation of the Russian Federation

6 On electronic signature. No. 63-FZ of 06.04.2011. KonsultantPlyus. https://clck.ru/3QH6dk

7 State Standard. (2012). Information technology. Methods and means of ensuring security. Guidelines for the identification, collection, receipt and storage of evidences provided in a digital form (GOST R ISO/IEC 27037-2014 (ISO/IEC 27037:2012)). Rosstandart. https://clck.ru/3QH6hR

8 State Standard. (2017). Forensic computer and technical expertise (GOST R 57429-2017). Rosstandart. https://clck.ru/3QH6ji

9 UUID is a universally unique identifier of digital data.

Secondly, there is a lack of competence of persons, who make video sound recordings; who carry out procedural recording of EE; who are involved as experts in order to confirm the accuracy of the recorded information; and the judges. Incompetence lies in a lack of understanding of the EE nature as a whole, as well as in the inability, in particular, to identify "potentially criminalistically significant information ... that does not and cannot have a direct causal relationship with the crime event, is not included in the subject of proof, but which is objectively necessary for the proper resolution of the case and contributes to solving diagnostic, classification and identification tasks" [10]. For example:

– Investigators, judges, and other participants in the process who do not have special knowledge tend to overly rely on the alleged "objectivity" of the video image, believing that it shows the facts as they really are ("naive realism"), since their personal experience is insufficient to form a critical attitude towards the perception of recorded audiovisual information.

– 37 % of the interrogated investigators do not know what the hash sum of the data contained in the file is; only one investigator uses the hash sum as a way to protect the file from modification (Shikhalieva, 2025). In investigative documentation, so rarely contain the hash sum of video and audio data that it cannot be considered a statistically significant event[11].

– During the examination, an expert did not take into account that, according to the audio file metadata, the audio was recorded using the iOS version, which appeared several months after the events recorded on the phonogram; another expert did not notice that the audio file content changed two days after the investigator drew up the protocol and recorded the audio file on an optical disc.

– The authors of the "Instructions for record keeping in the arbitration courts of the Russian Federation (first, appellate and cassation instances)"[12] not only lack understanding how the recording quality of a phonogram is assessed, but are also unable to correctly specify the unit of measurement of the recording information speed and the standard signal sampling rate: "The recording quality is 128 Kb/s, sampling rate 44 kHz, stereo mode". Apparently, the Instructions do not provide means of verifying recorded phonograms[13].

– Increasingly, videograms and videophonograms used in evidence have metadata or video- and audiodata distorted and (or) modified as a result of transmission using Internet messengers.

---

10 Yalyshev, S. A. (1999). Criminological registration: tutorial. Moscow: Academy for the management of the Russian Ministry of Internal Affairs. P. 37.

11 Based on over 30 years of the author's experience of providing phonovideoscopic expertise and studies.

12 Approved by Resolution of the Plenum of the Supreme Arbitration Court of the Russian Federation No. 100 of December 25, 2013. KonsultantPlyus. https://clck.ru/3QH6qE

13 Verification of phonograms is establishing the identity of two sets of sound data.

– "... a typical silent scene rounded up the 'tour' for cadets, young investigators and operations staff along several floors with hundreds of racks of identical equipment in the Rostelecom PJSC data center after the question "If your computer system is distributed in the cloud infrastructure of the data center, what and how will you inspect and exact here in accordance with the Criminal Procedural Code? Where will you keep the items exacted?" (Zemskova, Minakov, 2023).

The above emphasis on "potentially criminalistically significant information" is not accidental. The current level of development of digital signal processing technologies, including artificial intelligence, makes it possible to modify or fabricate PhVVphs without leaving any traces (Zubov, Zubova, 2023; Bodrov, Lebedeva, 2024). In this regard, while assessing the recorded information reliability, it is particularly important to establish the conformity of the PhVVphs content and technical characteristics with the circumstances of their creation, known and reflected in the procedural documents (Voznyuk, Denisov, 2017). For example, experts, with the participation of the author of this article, have repeatedly managed to establish the fact that the court session phonogram was replaced by another phonogram that had no traces of modification, but was recorded at another time in a different sound environment that did not correspond to the courtroom[14].

The third factor is the EE vulnerability, which manifests itself, among other things, in the following:

– Distortion, destruction, blocking of access to information, as well as loss, destruction or malfunction of the information carrier because of user errors, failure of technical and software tools of information systems, exposure to natural phenomena or other events, including those not aimed at changing information (GOST R 50922-2006[15]).

– A large set of methods and means of EE deliberate destruction or concealment: using both standard and special software, including malicious ones; by completely overwriting the hard disk; by formatting the media; by encryption or electromagnetic force exposure (GOST R 50922-2006).

– Difficulties in implementing measures to ensure the EE protection from intentional and unintended effects, including electromagnetic and (or) other physical effects, carried out, among other things, for criminal purposes (GOST R 50922-2006). "... (D)ue to the high volatility of information in digital media and systems, the detection of digital traces of a crime during repeated or additional inspection over time will in most cases be unlikely" (Zemskova, Minakov, 2023).

Fourthly, the "paper" recording of evidentiary information adopted in procedural practice does not correspond to the PhVVphs nature; the latter contain information about

[14] Laboratory of audiovisual documents. VKontakte. https://clck.ru/3QH6ra

[15] State Standard. (2006). Information protection. Key terms and definitions (GOST R 50922-2006). Rosstandart. https://clck.ru/3QH6uJ

video and audio events in duration that one cannot view as a whole at any given time and adequately reflect in a written document. In this regard, an expert is often assigned to establish the verbatim content of the PhVVphs and provide a so-called storyboard – hard copies of the video images with a textual description of their content. This does not allow one to fully convey "the intonation and nuances of a person's presentation of thoughts, the expressiveness of speech and the tone of conversation, facial expressions, gestures, emotional state, attitudes of the video participants to the phrases, actions, and reactions of other participants in the events" (Vlasov, 2024).

2. Methodology for the formation of the conceptual apparatus and classification of electronic evidences

Obviously, one may determine the place of digital PhVVphs in the EE series only if there is a system of fully encompassing notions, definitions and terms related to the area under consideration and constituting the conceptual apparatus of the EE.

A serious obstacle to the formation of the EE conceptual apparatus is the existence of many inconsistent descriptions of the same concept. A clear example of this heterogeneity is the different interpretations of the concept of "electronic document" in legislation (see above) and in the current state standards:

– "electronic document: a document on a machine-readable medium, requiring computer equipment to use"[16];

– "electronic document: an information object consisting of two parts:

– a prop containing identifying attributes (title, time and place of creation, information about the author, etc.) and an electronic digital signature,

– meaningful, including textual, numerical and (or) graphical information that is processed as a single whole"[17];

– "electronic document: a form of presentation of a document as a set of interrelated implementations in an electronic environment and their corresponding interrelated implementations in a digital environment"[18];

– "electronic document: a document whose information is presented in electronic form"[19];

---

16 State Standard. (2001). Electronic publications. Main types and issuance information (GOST 7.83-2001). Rosstandart. https://clck.ru/3QH6wz

17 State Standard. (2001). Information technologies to support product lifecycle. Terminological dictionary. Part 1. Stages of the product life cycle (GOST R 50.1.031-2001). Rosstandart. https://clck.ru/3QH6za

18 State Standard. (2004). Information technology. Electronic information exchange. Terms and definitions (GOST R 52292-2004). Rosstandart. https://clck.ru/3QH77t

19 State Standard. (2013). System of standards in information, librarianship, and publishing. Record keeping and archiving. Terms and definitions (GOST R 7.0.8-2013). Rosstandart. https://clck.ru/3QH7AR

– "electronic document: a document in digital form, the use of which requires computer means or other specialized devices for reproducing text, sound, and images"[20].

The variety of definitions is largely due to the fact that individual standards and laws have a limited scope of application and are focused on solving problems in specific areas of human activity. Therefore, it is logical to begin the formation of the EE conceptual apparatus by defining the main task for which it is used. This task is to ensure a uniform understanding and interpretation of the generic and specific characteristics of EE, the relationships and processes formed or applied in the collection, verification and evaluation of evidentiary information, including using the means and methods of forensic examination.

Given that the techniques and methods used when collecting, storing, processing, transmitting and using data constitute information technology[21], it seems logical to use definitions already contained in the state standards in the field of information technology (IT) for the EE conceptual apparatus[22].

Currently, there are several dozen such standards. The following are of the greatest interest in this study:

– GOST 15971-90 Information processing systems. Terms and definitions.

– GOST 13699-91 Recording and reproduction of information. Terms and definitions.

– GOST R 52292-2004 Information technology. Electronic information exchange. Terms and definitions.

– GOST R ISO/IEC 27037-2014 (ISO/IEC 27037:2012) Information technology. Methods and means of ensuring security. Guidelines for the identification, collection, receipt and storage of evidences provided in a digital form[23].

– GOST 33707-2016 (ISO/IEC 2382:2015) Information technologies. Dictionary.

The above standards use the "modern approach to information technology specification based on distinguishing two different aspects of phenomena: social (in this case, purpose, information, document, etc.) and technological (in this case, media, format, data, etc.)" (GOST R 52292). This is quite consistent with two different but interrelated aspects of EE fixation (Belkin, 2007). The procedural side is aimed at forming a legally binding evidence framework by reflecting the factual data, discovered by the investigator, in the procedural documents. The forensic side primarily touches upon the means and methods used at various stages of the detection and consolidation of evidentiary information.

---

20 State Standard. (2013). System of standards in information, librarianship, and publishing. Electronic publications. Main types and issuance information (GOST R 7.0.83-2013). Rosstandart. https://clck.ru/3QH7CR

21 State Standard. (1990). Information technology. Set of standards for automated systems. Terms and definitions (GOST 34.003-90). Rosstandart. https://clck.ru/3QH7EK

22 Not to be confused with the " System of standards in information, librarianship, and publishing".

23 This standard is recommended by the UN Office on Drugs and Crime for use in the investigation of cybercrimes. https://clck.ru/3QH7Pr

These stages include[24]:

1. Identifying EE – search, recognition and documentation of potential EE. During the identification process, information carriers and processing devices are identified that may contain potential EE.

2. Collecting EE – placing media with EE in a controlled environment for subsequent extraction of evidentiary information.

3. Receiving EE – creating a copy of EE.

4. Storing EE – ensuring the protection of EE from changes (falsification, damage, etc.).

5. Analyzing EE – in-depth research in order to identify evidentiary information.

6. Presenting (summarizing and explaining) the discovered factual data in a procedural document.

It is important that at all these stages "not only the evidentiary information per se is captured, but also information about the ways, methods and means of obtaining it as a necessary condition for its admissibility in the case" (Belkin, 2007).

It should also be noted that currently in Russia there is still no model for working with digital evidence during investigations, common for various law enforcement agencies.

Most of the standardized IT terms characterizing the technological/forensic side of collecting EE can be applied in the conceptual framework of EE without any changes. Missing generic and specific concepts related directly to IT can be formed by concretizing and adapting existing basic IT concepts based on "analyzing and generalizing the properties and features of objects and identifying the characteristics describing concepts" (GOST R 50.1.075[25]) (Fig. 1), including taking into account the relationship of the "information" and "data" concepts shown in Fig. 2.

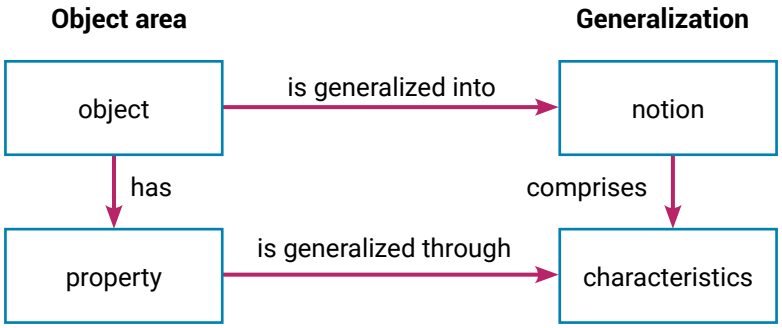


Fig. 1. Order of forming new concepts according to GOST R 50.1.075

[24] A typical integrated model for working with digital evidence is presented, para. 1-4 of which correspond to the recommendations of GOST R ISO/IEC 27037, para. 5 and 6 – to the model based on the US FBI protocol (Reedy, 2022).

[25] State Standard. (2011). Elaboration of standards for terms and definitions (GOST R 50.1.075-2011). Rosstandart. https://clck.ru/3QH7T9

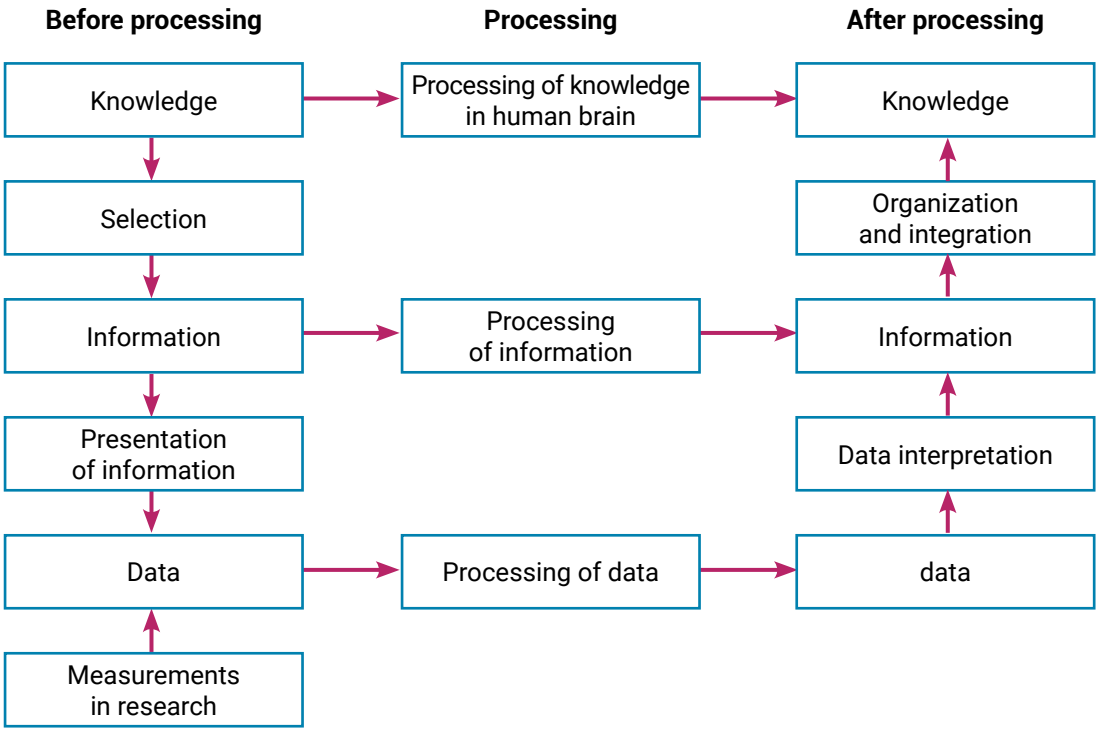


Fig. 2. A diagram reflecting the relationship between the concepts of "knowledge", "information" and "data" in accordance with ISO/IEC 2382-1:1993[26]

Using these standards and principles, it is not difficult to formulate terms and definitions universal for all types of legal proceedings, forming the basis of the EE conceptual apparatus.

GOST R 52292 provides the following definitions of "data" and "electronic environment":

– "data[27]: a formalized representation of information suitable for communication, interpretation or processing <...>;

– analog data: data represented by a physical quantity that is considered a continuous variable and whose value is directly proportional to the data or a suitable data function <...>;

– discrete data (symbolic data): data represented by symbols <...>;

– electronic environment: the environment of technical devices (hardware) operating on the basis of physical laws and used in information technology for the processing, storage and transmission of data"[28].

[26] ISO/IEC 2382-1:1993 Information technology. Dictionary. Part 1. Basic terms. Substituted with ISO/IEC 2382:2015. https://clck.ru/3QH7fj

[27] Depending on the type of information, the data can be audio, video, etc.

[28] State Standard. (2004). Information technology. Electronic information exchange. Terms and definitions (GOST R 52292-2004). Rosstandart. https://clck.ru/3QH77t

From these definitions, it follows that electronic evidence should be understood as data containing evidentiary information, stored or transmitted in a form suitable for human perception using information technology and electronic equipment.

The electronic technology mentioned in the definition includes not only computing facilities, but also electronic devices used for processing, recording, converting or transmitting information or energy using electronic components and principles of electronics. For example, for a person to perceive the sound information contained in a digital phonogram or video phonogram, it is not enough to have a DAC[29] (computing device) and a codec (information technology); it requires electronic devices designed to amplify an electrical signal and convert it into sound waves of various frequency and power.

Information technology is the techniques and methods of using computer technology in performing the functions of collecting, storing, processing, transmitting and using data (GOST 34.003-90).

It follows from the definitions of GOST R 52292 that EE can be represented in two types (Fig. 3):

– analog, in which a physical quantity takes on an infinite set of values that change continuously; and

– discrete, meaning that data exist in the form of discrete symbols, each of which can take one of a finite number of values.

That corresponds to Interpol's position on this issue: "Electronic evidence is a derivative term for two types of evidence: analog evidence and digital evidence" (Reedy, 2022).

Accordingly, digital evidence containing evidentiary information is data stored or transmitted in the form of binary code (GOST R ISO/IEC 27037); the term refers to electronic discrete evidence. The same class of evidence includes string and logical data, for example, those displayed on the screen of a voice recorder or smartphone (smartphone IMEI; phonogram title; time and geographical coordinates of the sound recording or video location; real-time clock readings of the recording device; phonogram duration; position (on/off) of the trigger or AGC[30] controls).

Thus, a digital phonogram containing evidentiary information belongs to the class of electronic discrete digital evidence. It is digital audio data stored on a tangible medium, obtained as a result of:

– digital sound recording – digital recording of sound, or sound information, coming from a primary source or a device for reproducing sound information (Fig. 3);

---

[29] DAC (digital-analog converter) – a device for converting digital data into an analog signal.

[30] AGC – automatic signal gain control.curcuit.

– generation (synthesis) of sound using algorithms and methods of digital signal processing.

The importance of distinguishing two ways of creating a digital phonogram is due to the following:

– The need to distinguish between the actual sound recording and recording on a digital audio data carrier. The latter can be either one of the stages of sound recording (Fig. 3), or a self-sufficient process carried out in order to copy digital audio data or save the generated data (see below).

– The fact that sound synthesis can be performed using previously recorded audio signals or their components indicating time and frequency, as well as on the basis of a mathematical or generative[31] model, without using the sound recording process at all stages of phonogram creation.

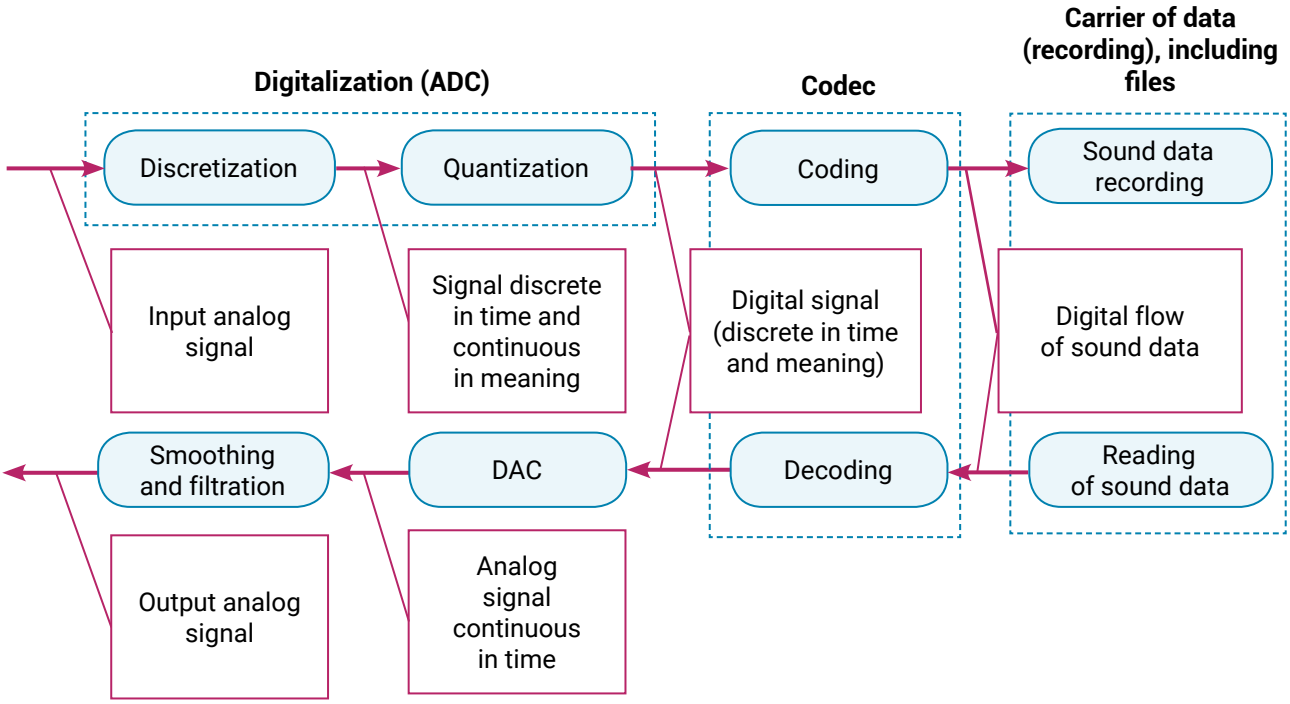


Fig. 3. Digital sound recording and sound reproduction

Source: (Zubov, 2020).

Digital audio data should be understood as the result of digitization and encoding of audio signals, presented in a form suitable for communication, interpretation or processing using electronic devices and information technologies. The recording of digital audio data on a media can be accompanied by the creation of files and metadata.

The need to mention “analog phonograms” is due, in particular, to the fact that there are aircraft still in operation, in which flight data and crew negotiations are recorded with

[31] The generative model creates training-like data based on statistical patterns, but not based on physical laws.

analog tape recorders (on magnetic tape or wire); stored in archives, there are analog phonograms and videophonograms recorded on magnetic tape, film, discs, etc.

It also follows from the above that not all currently existing phonograms can be classified as EE. For example, to record and reproduce mechanical (by recording method) analog phonograms on discs, rollers, etc., the use of electronic equipment and information technology is not necessary.

Obviously, it is not difficult to form similar definitions of a videogram or videophonogram and the data contained in them.

Thus, a videophonogram should be called digital video and audio data stored on a tangible medium, obtained as a result of:

– digital video sound recording – synchronous digital recording of video and sound, or audiovisual information coming from the primary source or a reproduction device;

– generation (synthesis) of video images and sound using algorithms and methods of digital signal processing.

Let us focus separately on data carriers, which are material objects (including a physical field) intended for recording and storing data, which, due to their tangibility, are often classified as physical evidence in procedural documents. It is advisable to classify media: by the recording method (mechanical, magnetic, optical, electronic, etc.); by the form of recorded data representation (analog, digital, etc.); and by the type of information (video, audio, text, etc.). In this case, for example, a music CD is an optical carrier of digital audio data; an ordinary tape recorder with a magnetic phonogram is a magnetic carrier of analog audio data; a hard disk with digital phonograms is a magnetic carrier of digital audio data; a flash drive is a solid-state carrier.

A special case of a data carrier is a "recording medium", or "a physical body used during recording to store information signals in it or on its surface"[32], for example, a tape cassette or an optical disc.

The above example with the classification of a music CD shows that not all digital data carriers are electronic carriers. The latter should include only electronic devices of the appropriate purpose that operate with their own controller[33]: a flash drive; a hard disk; a hardware RAID array; a network storage, etc.

Apparently, it is not easy for a nonprofessional to determine whether a data carrier belongs to a certain class. Therefore, in procedural documents drawn up by a nonprofessional, it is quite acceptable to indicate, along with other identifying

---

[32] State Standard. (1991). Information recording and reproduction. Terms and definitions (GOST 13699-91). Rosstandart. https://clck.ru/3QH7or

[33] A controller (in electronic engineering) is a specialized electronic device (or its assembly) designed to automatically control a technical object (process) according to a set algorithm (program).

information, only the type of media (a hard or optical disk; a flash drive; a tape recorder) and the characteristics of its contents (an audio or video file, a magnetic or digital phonogram and so on). The classification and explication of data carriers acquires the greatest importance at the stage of assessing the admissibility and reliability of evidence, including using the means and methods of forensic examination.

It is also important to keep in mind the following significant feature of digital PhVVphs. They can be presented in a virtual form, for example, a videophonogram published on the YouTube[34] Internet service, or files with PhVVphs in a cloud storage. Therefore, at the stage of such PhVVphs' identification, their carrier cannot always be determined, and to use PhVVphs as evidence, it will be necessary to copy or export the data to an alienated medium.

Hence, the technical side of the standard procedure for exporting data from virtual to alienated media includes a number of sequential operations that can take place automatically, including without the user's knowledge and control. These may include:

– extracting data from the source environment (database, information system, etc.);

– converting data into a format which allows them to be imported and used in another system or environment;

– actual storage of data on alienated media for their further use or processing.

In other words, the PhVVphs obtained as a result of export are not always copies of those recorded on virtual media.

In this regard, it is advisable to identify a primary carrier to which audio and video signals coming directly from the original source were recorded. In other words, this is the first tangible object on which specific data were recorded. The secondary carrier is that on which the data were stored as a result of copying or exporting data from the primary or another secondary media. The primary carrier can be either embedded (inalienable) or removable (alienable); the secondary one is alienable, as a rule.

Both primary and secondary carriers can also be virtual at the same time, which the user can access via the Internet or in a similar way.

We also consider important to mention the definition of a "digital evidence copy" as a created copy of a digital evidence and a means of verifying it, which is given in GOST R ISO/IEC 27037. It follows that a copy of a digital phonogram containing evidentiary information can only be considered a phonogram obtained as a result of file-based or bitwise copying, the conformity of which can be verified either using the verification function or in another acceptable way. In the English-language specialized literature, this is also called a "forensic copy".

[34] The foreign person owning the YouTube informational resource violates the legislation of the Russian Federation.

Naturally, all these definitions are not "carved in stone" and can be replaced with synonymous ones that do not distort the essence of the described properties, processes and phenomena. For example, the verification of the immutability of files by establishing the identity of two sets of data contained in them is called "verification" in GOST R ISO/IEC 27037 and "authentication" in GOST R 57429, which does not change the meaning and content of the procedure.

3. International experience

Currently, the "branch of criminology that applies legal issues to information and communication technologies and digital devices"[35] , commonly referred to as Digital forensics, is recognized as an independent scientific discipline by many international and national organizations. These include the United Nations Office on Drugs and Crime, Interpol, the European Network of Forensic Science Institutes (ENFSI), the European Union Agency for Cybersecurity (ENISA), the American Academy of Forensic Sciences (AAFS), the Organization of Scientific Industry Committees (OSAC)[36], the UK Forensic Science Regulator, the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC). The fundamental sciences and basic scientific directions for various subdisciplines of digital forensics currently include: biology, physics, mathematics, linguistics, as well as computer science, computer engineering, image science, acoustics, anthropology, statistics, and data science (Reedy, 2020; Rybaczewska & Sparks, 2022).

Publicly available publications of the above organizations provide a rather comprehensive picture of the current state of digital forensics, its methods and procedures related to working with digital evidence. It should be noted that the features of working with the PhVVphs are not specified in the listed documents.

In 2020, a manual "Cybercrime"[37] consisting of 14 modules was published, as a result of the joint work of the United Nations Office on Drugs and Crime and leading experts from more than 25 countries around the world. Module 4 of this manual, "Introduction to digital forensics", provides an overview of the current state of digital forensics, in particular, the digital forensics standards, the process of examining digital evidence and general practical methods of expert research, as well as best practices in the field of digital forensics.

---

35 United Nations Office on Drugs and Crime. (2020). "Cybercrime" – a series of university modules. https://clck.ru/3QH7sy

36 Adopted by the US National Institute of Standards and Technology (NIST) for the development of specialized standards of forensic examination.

37 United Nations Office on Drugs and Crime. (2020). "Cybercrime" – a series of university modules. https://clck.ru/3QH7sy

An analysis of trends, problems, and achievements of Interpol and law enforcement agencies in different countries in the field of collecting, analyzing, and using digital evidence in crime investigations is provided in the Interpol review of digital evidence for 2016–2019 and 2019–2022 (Reedy, 2020; 2022; Tripathi & Meshram, 2022; Insa, 2007).

In 2019, Interpol published Global Guidelines for Digital Forensics Laboratories[38]. The document is a guide to the creation, management and operation of digital forensics laboratories in accordance with common standards that ensure the admissibility of electronic evidence in courts, including international ones.

The 2014 ENISA guide for first responders to computer incidents[39] focuses on how to handle digital evidence, starting with arrival at the crime scene and ending with the assessment and presentation of digital evidence.

The Best Practice Manual of the European Network of Forensic Science Institutes (ENFSI), devoted to conducting digital forensic research (version 1, 2015)[40], reflects the standard procedure of forensic examination of digital evidence, standards and universal methods of expert research, as well as best practices in the field of digital forensics, including staff training. Taken together, these should ensure the reliability and comparability of the results of forensic examinations.

The NIST IR 8387 (September 2022) report (Guttman et al., 2022; Turner, 2005; Romaniuk, 2024), prepared in partnership with the US National Institute of Justice (NIJ) and aimed at professionals in evidence management, provides practical recommendations for preserving digital evidence and describes their unique features.

The key problems faced by law enforcement specialists include data encryption, cloud services, distributed storage, the Internet of Things, artificial intelligence, a shortage of qualified specialists, and differences in national legislations. The main recommendations include the harmonization of legal norms, investments in training specialists and equipping laboratories, and the development of compatible technologies for examining digital evidence.

It is emphasized that “every case involving digital evidence poses new challenges that digital evidence specialists must be able to solve. A future digital evidence specialist must have the knowledge and skills to solve forensic issues in a specific case” (Reedy, 2020; An, 2017; Awwad, 2025; Hosmer, 2006; Maurer, 2004).

---

38 Interpol. (2019). INTERPOL Global guidelines for digital forensics laboratories. https://clck.ru/3QH7zA

39 Electronic evidence – a basic guide for First Responders Good practice material for CERT first responders. (2014). European Union Agency for Network and Information Security.

40 Best Practice Manual for the Forensic Examination of Digital Technology ENFSI-BPM-FIT-01 Version 01 - November 2015. (2016). ENFSI. https://clck.ru/3QH83b

It should be mentioned that, in addition to GOST R ISO/IEC 27037 adapted to Russian conditions, ISO/IEC published additional international standards that have no Russian analogues. They cover reliability of digital forensic examination tools and methods – ISO/IEC 27041:2015 "Information technology. Security techniques. Guidance on assuring suitability and adequacy of incident investigative method", as well as the stages of research and interpretation of the digital forensic examination process – ISO/IEC 27042:2015 "Information technology. Security techniques. Guidelines for the analysis and interpretation of digital evidence".

Thus, the world has accumulated a wealth of experience in developing regulations – instructions, manuals, as well as standards and training materials on the creation and operation of digital forensics laboratories and working with digital evidence in the investigation of crimes. At the same time, the concept of "electronic evidence" is practically not used in modern regulatory documents and standards, since the features of studying analog evidence have long been known and studied and, together with digital evidence, they constitute an array of "electronic" evidence.

Conclusions

Digital phonograms, videograms, and videophonograms occupy a significant place in the EE system, representing highly vulnerable sources of audiovisual information that require a specialized approach to their recording, verification, and evaluation in court proceedings.

The lack of clear definitions and classifications of EE and PhVVphs in regulatory legal acts leads to legal uncertainty, errors in procedural practice and a decreased effectiveness of using such evidence in general.

The proposed methodology for the formation of the conceptual apparatus of the EE in general and PhVVphs in particular, based on existing state standards in the field of information technology, makes it possible to create universal terms and definitions adapted for all types of legal proceedings.

Further research in this area should be aimed at developing utmost clear and detailed recommendations, guidelines and instructions for experts and investigators on the identification, collection, receipt, preservation and analysis of EE, including using foreign experience.

In the future, it is necessary to improve the procedural rules, including the introduction of mandatory requirements for the competence of specialists and their mandatory involvement in the earliest stages of investigation.

References

An, S. S. (2017). The admissibility of digital evidence. *Korean Lawyers Association Journal*, *66*(1), 5–56. https://doi.org/10.17007/klaj.2017.66.1.001

Awwad, A. (2025). Digital evidence in forensic accounting: A study in Saudi Arabia. *Journal of Accounting and Finance in Emerging Economies*, *5*(1), 23–31. https://doi.org/10.1177/097215092501001

Belkin, A. R. (2007). *Theory of proving in criminal judicial procedure*. Moscow: Norma. (In Russ.).
Bodrov, N. F., & Lebedeva, A. K. (2024). Analysis of the case law establishing circumstances of illegal distribution of generative content created using artificial intelligence. *Legal Studies*, *11*. (In Russ.). https://doi.org/10.25136/2409-7136.2024.11.72540
Cheretskikh, A. V. (2023). Digital (electronic) evidence in criminal proceedings. *Legal Order: History, Theory, Practice*, *4*(39), 110–117. (In Russ.). https://doi.org/10.47475/2311-696X-2023-39-4-110-117
Guttman, B., White, D. R., & Walraven, T. (2022). Digital Evidence Preservation Considerations for Evidence Handlers. *NIST Interagency Report NIST IR 8387*. https://doi.org/10.6028/NIST.IR.8387
Hosmer, C. (2006). Digital evidence bag. *Communications of the ACM*, *49*(2), 69–70. https://doi.org/10.1145/1113034.1113072
Insa, F. (2007). The admissibility of electronic evidence in court (A.E.E.C.). *Computer Law & Security Review*, *23*(5), 409–418. https://doi.org/10.1016/j.clsr.2007.07.002
Malyk, A. V. (2023). Formation and nature of electronic evidence. *Proceedings of Voronezh State University. Series: Pravo*, *3*(54), 45–51. (In Russ.). https://doi.org/10.17308/law/1995-5502/2023/3/45-51
Maurer, U. (2004). New approaches to digital evidence. *Proceedings of the IEEE*, *92*(6), 933–947. https://doi.org/10.1109/jproc.2004.827358
Politsan, D. A. (2022). "Digital" and "Electronic" evidence – pro et contra: problems of terminology. *Rossiyskiy sudya*, *7*, 38–44. (In Russ.). https://doi.org/10.18572/1812-3791-2022-7-38-44
Reedy, P. (2020). Interpol review of digital evidence for 2016–2019. *Forensic Science International: Synergy*. https://doi.org/10.1016/j.fsisyn.2020.01.015
Reedy, P. (2022). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*. https://doi.org/10.1016/j.fsisyn.2022.100313
Romaniuk, V. V. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Problems of Legal Regulation*, *59*(2), 47–56. https://doi.org/10.32782/2524-0374/2024-2-10
Rybaczewska, M., & Sparks, L. (2022). Digital evidence and online consumer engagement. *Journal of Retailing and Consumer Services*, *65*, Article 102889. https://doi.org/10.1016/j.jretconser.2022.102889
Shikhaliyeva, S. Z. (2025). The absence of a hash sum as a procedural error arising in a forensic examination when analysing objects in a digital form. *The Rule-Of-Law State: Theory and Practice*, *21.1*(79), 256–263. (In Russ.). https://doi.org/10.33184/pravgos-2025.1.28
Tripathi, S., & Meshram, B. B. (2022). Digital evidence for database tamper detection. *Advances in Multidisciplinary and Scientific Research Journal Publication*, *1*(1), 185–190. https://doi.org/10.22624/aims/crp-bk3-p30
Turner, P. (2005). Unification of digital evidence from disparate sources (Digital Evidence Bags). *Digital Investigation*, *2*(3), 223–228. https://doi.org/10.1016/j.diin.2005.07.001
Vlasov, O. O. (2024). Classification of tasks for forensic video analysis. *Theory and Practice of Forensic Science*, *19*(2), 14–25. (In Russ.). https://doi.org/10.30764/1819-2785-2024-2-14-25
Voronin, M. I. (2021). Characteristics of electronic (digital) evidence assessment. *Actual Problems of Russian Law*, *8*(129), 118–128. (In Russ.). https://doi.org/10.17803/1994-1471.2021.129.8.118-128
Voznyuk, M. A., & Denisov, Yu. A. (2017). Forensic diagnostics of the circumstances of digital video and audio production: analytical review. *Theory and Practice of Forensic Science*, *12*(1), 48–71. (In Russ.). https://doi.org/10.30764/64/1819-2785-2017-12-1-48-71
Zemskova, A. V., & Minakov, S. S. (2023). Features of the use of tools for searching and documenting computer information during investigative actions on inspection. *Vestnik economicheskoy bezopasnosti*, *2*, 74–85. (In Russ.). https://doi.org/10.24412/2414-3995-2023-2-74-85
Zubov, G. N. (2020). Actualizing the concept of "special technical means for covert obtaining of information" in the photovideoscopic expertise. *Vestnik kriminalistiki*, *2*(74), 52–60. (In Russ.).
Zubov, G. N., Timoshenko, A. A. (2014). Using digital audio- and videophonograms in proving. *Ugolovniy protsess*, *2*(110), 52–61. (In Russ.).
Zubov, G. N., Zubova, P. I. (2023). Falsification of audio information using artificial intelligence technologies. Features of technical research. *Vestnik kriminalistiki*, *3*(87), 5–26. (In Russ.).

Author information

German N. Zubov – independent researcher, independent legal expert
Address: 10A Energetikov Str., Saint Petersburg, Russia
E-mail: hzubov@yandex.ru
ORCID ID: https://orcid.org/0000-0002-9504-1715
RSCI Author ID: https://www.elibrary.ru/author_items.asp?spin=5528-9035

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – September 25, 2025
Date of approval – October 8, 2025
Date of acceptance – December 20, 2025
Date of online placement – December 25, 2025

Научная статья
УДК 34:004:343.14:343.98.062:343.98.063
EDN: https://elibrary.ru/qjhwgw
DOI: https://doi.org/10.21202/jdtl.2025.25

Место цифровых фонограмм, видеограмм и видеофонограмм в системе электронных доказательств: теоретико-методологические основы классификации

Герман Николаевич Зубов

Независимый исследователь, Санкт-Петербург, Россия

Ключевые слова

видеограмма,
видеофонограмма,
доказательства,
право,
судопроизводство,
фонограмма,
цифровая криминалистика,
цифровые технологии,
экспертиза,
электронные
доказательства

Аннотация

Цель: исследование направлено на определение места цифровых фонограмм, видеограмм и видеофонограмм в системе электронных доказательств в российском судопроизводстве с формированием единого понятийного аппарата и классификационной системы для обеспечения эффективного использования в процессуальной практике.

Методы: методологическую основу исследования составляют всеобщий диалектический метод познания, общенаучные методы (описание, сравнение, обобщение, моделирование, анализ, синтез) и частнонаучные методы. Особое внимание уделено системно-структурному анализу нормативно-правовых актов, государственных стандартов в области информационных технологий, международных документов, регламентирующих работу с цифровыми доказательствами. Применены методы криминалистического исследования, формально-юридический метод толкования норм процессуального законодательства, компаративный анализ зарубежного опыта регулирования электронных доказательств.

Результаты: в ходе исследования выявлены и систематизированы ключевые причины правовой неопределенности электронных доказательств: многообразие форм представления, высокая уязвимость данных, недостаточная компетентность субъектов доказывания, несоответствие традиционным методам фиксации доказательственной информации. Разработана оригинальная классификация электронных доказательств и цифровых фонограмм, видеограмм, видеофонограмм с использованием критериев формы представления данных, способа записи, характера носителей информации. Сформулированы универсальные определения базовых понятий: электронные доказательства, цифровые доказательства, цифровая фонограмма, видеофонограмма,

носители данных, копия цифрового доказательства. Обоснована необходимость гармонизации процессуальных норм на основе государственных стандартов информационных технологий и международного опыта.

Научная новизна: впервые разработана комплексная методология формирования понятийного аппарата и классификации электронных доказательств, основанная на интеграции государственных стандартов информационных технологий с криминалистическими и процессуальными аспектами фиксации доказательственной информации. Введены универсальные термины и определения, отсутствующие в действующем российском законодательстве, адаптированные для всех видов судопроизводства с учетом специфики цифровой среды. Предложена типовая модель работы с цифровыми доказательствами, включающая этапы идентификации, сбора, получения, сохранения, анализа и представления. Обоснована категория цифровых фонограмм, видеограмм и видеофонограмм как подвида электронных дискретных цифровых доказательств.

Практическая значимость: результаты исследования могут быть использованы для совершенствования процессуального законодательства в части регламентации работы с электронными доказательствами, разработки ведомственных инструкций и практических рекомендаций для следователей, специалистов и экспертов по идентификации, сбору, фиксации, проверке и оценке цифровых доказательств. Предложенная классификация и понятийный аппарат способствуют унификации подходов к процессуальному оформлению электронных доказательств, минимизации процессуальных ошибок, повышению компетентности субъектов доказывания, обеспечению допустимости и достоверности цифровых фонограмм, видеограмм и видеофонограмм. Материалы исследования применимы в образовательном процессе при подготовке юристов, следователей, судебных экспертов, специализирующихся в области цифровой криминалистики.

Для цитирования

Зубов, Г. Н. (2025). Место цифровых фонограмм, видеограмм и видеофонограмм в системе электронных доказательств: теоретико-методологические основы классификации. *Journal of Digital Technologies and Law*, *3*(4), 636–659. https://doi.org/10.21202/jdtl.2025.25

Список литературы

Белкин, А. Р. (2007). *Теория доказывания в уголовном судопроизводстве*. Москва: Норма.

Бодров, Н. Ф., Лебедева, А. К. (2024). Анализ судебной практики установления обстоятельств в случаях противоправного распространения генеративного контента, созданного с помощью технологий искусственного интеллекта. *Юридические исследования*, *11*. EDN: https://elibrary.ru/TLSBYY. DOI: https://doi.org/10.25136/2409-7136.2024.11.72540

Власов, О. О. (2024). Классификация задач криминалистической экспертизы видеозаписей. *Теория и практика судебной экспертизы*, *19*(2), 14–25. EDN: https://elibrary.ru/XQEHZW. DOI: https://doi.org/10.30764/1819-2785-2024-2-14-25

Вознюк, М. А., Денисов, Ю. А. (2017). Экспертная диагностика обстоятельств изготовления цифровых видео- и звукозаписей: аналитический обзор. *Теория и практика судебной экспертизы*, *12*(1), 48–71. EDN: https://elibrary.ru/YHMVEL. DOI: https://doi.org/10.30764/64/1819-2785-2017-12-1-48-71

Воронин, М. И. (2021). Особенности оценки электронных (цифровых) доказательств. *Актуальные проблемы российского права*, *8*(129), 118–128. EDN: https://elibrary.ru/ncpirv. DOI: https://doi.org/10.17803/1994-1471.2021.129.8.118-128

Земскова, А. В., Минаков, С. С. (2023). Особенности применения инструментальных средств для поиска и документирования компьютерной информации в ходе следственных действий по осмотру. *Вестник экономической безопасности*, *2*, 74–85. EDN: https://elibrary.ru/hcvgtp. DOI: https://doi.org/10.24412/2414-3995-2023-2-74-85

Зубов, Г. Н. (2020). Актуализация понятия «специальные технические средства для негласного получения информации» в фоновидеоскопической экспертизе. *Вестник криминалистики*, *2*(74), 52–60. https://elibrary.ru/rnbdma

Зубов, Г. Н., Зубова, П. И. (2023). Фальсификация звуковой информации с использованием технологий искусственного интеллекта. Особенности технического исследования. *Вестник криминалистики*, *3*(87), 5–26. https://elibrary.ru/qvhfrw

Зубов, Г. Н., Тимошенко А. А. (2014). Использование в доказывании цифровых аудио и видеофонограмм. *Уголовный процесс*, *2*(110), 52–61. https://elibrary.ru/ruqikd

Малык, А. В. (2023). Формирование и природа электронных доказательств. *Вестник Воронежского государственного университета. Серия: Право*, *3*(54), 45–51. EDN: https://elibrary.ru/atlajw. DOI: https://doi.org/10.17308/law/1995-5502/2023/3/45-51

Полициан, Д. А. (2022). «Цифровое» и «электронное» доказательство – pro et contra: проблемы терминологии. *Российский судья*, *7*, 38–44. EDN: https://elibrary.ru/fvlsvs. DOI: https://doi.org/10.18572/1812-3791-2022-7-38-44

Черецких, А. В. (2023). Цифровые (электронные) доказательства в уголовном процессе. *Правопорядок: история, теория, практика*, *4*(39), 110–117. EDN: https://elibrary.ru/ptaemv. DOI: https://doi.org/10.47475/2311-696X-2023-39-4-110-117

Шихалиева, С. З. (2025). Отсутствие хэш-суммы как процессуальная ошибка, возникающая в судебной экспертизе при исследовании объектов в цифровой форме. *Правовое государство: теория и практика*, *21.1*(79), 256–263. EDN: https://elibrary.ru/bntuwa. DOI: https://doi.org/10.33184/pravgos-2025.1.28

An, S. S. (2017). The admissibility of digital evidence. *Korean Lawyers Association Journal*, *66*(1), 5–56. https://doi.org/10.17007/klaj.2017.66.1.001

Awwad, A. (2025). Digital evidence in forensic accounting: A study in Saudi Arabia. *Journal of Accounting and Finance in Emerging Economies*, *5*(1), 23–31. https://doi.org/10.1177/097215092501001

Hosmer, C. (2006). Digital evidence bag. *Communications of the ACM*, *49*(2), 69–70. https://doi.org/10.1145/1113034.1113072

Maurer, U. (2004). New approaches to digital evidence. *Proceedings of the IEEE*, *92*(6), 933–947. https://doi.org/10.1109/jproc.2004.827358

Guttman, B., White, D. R., & Walraven, T. (2022). Digital Evidence Preservation Considerations for Evidence Handlers. *NIST Interagency Report NIST IR 8387*. https://doi.org/10.6028/NIST.IR.8387

Insa, F. (2007). The admissibility of electronic evidence in court (A.E.E.C.). *Computer Law & Security Review*, *23*(5), 409–418. https://doi.org/10.1016/j.clsr.2007.07.002

Reedy, P. (2020). Interpol review of digital evidence for 2016–2019. *Forensic Science International: Synergy*. https://doi.org/10.1016/j.fsisyn.2020.01.015

Reedy, P. (2022). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*. https://doi.org/10.1016/j.fsisyn.2022.100313

Romaniuk, V. V. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Problems of Legal Regulation*, *59*(2), 47–56. https://doi.org/10.32782/2524-0374/2024-2-10

Rybaczewska, M., & Sparks, L. (2022). Digital evidence and online consumer engagement. *Journal of Retailing and Consumer Services*, *65*, Article 102889. https://doi.org/10.1016/j.jretconser.2022.102889

Tripathi, S., & Meshram, B. B. (2022). Digital evidence for database tamper detection. *Advances in Multidisciplinary and Scientific Research Journal Publication*, *1*(1), 185–190. https://doi.org/10.22624/aims/crp-bk3-p30

Turner, P. (2005). Unification of digital evidence from disparate sources (Digital Evidence Bags). *Digital Investigation*, *2*(3), 223–228. https://doi.org/10.1016/j.diin.2005.07.001

Сведения об авторе

Зубов Герман Николаевич – независимый исследователь, независимый судебный эксперт
Адрес: 195027, Россия, г. Санкт-Петербург, пр. Энергетиков, 10а
E-mail: hzubov@yandex.ru
ORCID ID: https://orcid.org/0000-0002-9504-1715
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?spin=5528-9035

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 25 сентября 2025 г.
Дата одобрения после рецензирования – 8 октября 2025 г.
Дата принятия к опубликованию – 20 декабря 2025 г.
Дата онлайн-размещения – 25 декабря 2025 г.

Research article
UDC 34:004:340.1:004.8:004.051
EDN: https://elibrary.ru/uiujcv
DOI: https://doi.org/10.21202/jdtl.2025.26

Explainable Artificial Intelligence and Legal Ethos: Developing Key Performance Indicators for 'G20 Giants'

Neelkanth Bhatt ✉
Government Engineering College, Rajkot, India

Jaikishen Nathalal Bhatt
Employees' State Insurance Corporation, Ahmedabad, India

Keywords

algorithmic transparency,
artificial intelligence,
criminal justice,
digital technologies,
economic development,
environmental sustainability,
ethics,
explainable artificial intelligence,
law,
public interest

Abstract

Objective: to study the "right to explanation" in the context of the PEEC doctrine (public interest, environmental sustainability, economic development, criminal justice) in order to develop key performance indicators reflecting the socio-cultural characteristics of different countries and ensuring adaptability, transparency and cultural relevance in the regulation of explainable artificial intelligence.

Methods: the research uses a unique methodological approach that combines the iterative processes of soft systems methodology with a theoretical framework based on the PEEC principles. Such integration makes it possible to comprehensively study the social, economic, political and legal regimes of the 'G20 Giants' – the United States of America, the Federal Republic of Germany, Japan, the Republic of India, the Federal Republic of Brazil and the Russian Federation – when designing key performance indicators. The proposed key performance indicators are applicable to assess the transparency and accountability of artificial intelligence systems, simplifying data collection and practical implementation in various cultural contexts. The developed model corresponds to the actual social needs in decision-making using artificial intelligence technologies.

✉ Corresponding author

Results: the study proposes a new legal model for regulating explainable artificial intelligence based on a system of key performance indicators. In addition to eliminating the problems of regulating explainable artificial intelligence in various cultural, ethical and legal fields, this model ensures that the system of regulating explainable artificial intelligence properly takes into account anthropocentric aspects, since it is focused on unlocking the true potential of artificial intelligence. The proposed approach promotes the most effective use of artificial intelligence technologies for the benefit of society in the perspective of sustainable development.

Scientific novelty: the work applies a unique scientific approach that takes into account cultural, ethical, socio-economic and legal differences when developing a legal framework for regulating explainable artificial intelligence. This allows adapting the legal framework to various national conditions, while contributing to responsible management of artificial intelligence with a check-and-balance system.

Practical significance: the results obtained make it possible to use the proposed legal model in the practical activities of government agencies and developers of artificial intelligence systems to ensure transparency and explainability of technologies. Effective adjustment of the proposed key performance indicators, taking into account the specifics of states, will optimize them for universal use. Although all five key performance indicators are relevant for the 'G20 Giants', their relative significance depends on the socio-cultural and legal conditions of a particular state. Further research should cover a wider range of issues, including other developed and developing countries, in order to adapt the regulation of explainable artificial intelligence to various national and global requirements.

For citation

Bhatt, N., & Bhatt, J. N. (2025). Explainable Artificial Intelligence and Legal Ethos: Developing Key Performance Indicators for 'G20 Giants'. *Journal of Digital Technologies and Law, 3*(4), 660–676. https://doi.org/10.21202/jdtl.2025.26

Contents

Introduction

The accountability, transparency and the legal liability of Artificial Intelligence (AI) systems have also evolved with the growing usage of these systems due to their complexities and autonomy. In cases of AI failures, assigning responsibilities and understanding how AI systems make decisions has brought to the forefront the question of its "explainability" (Gilpin et al., 2018; Hacker et al., 2020). To address this concern, the EU's General Data Protection Regulation (GDPR) allows individuals to seek insights into decisions of AI systems (Gilpin et al., 2018). Conversely, for a country like India having complex and heterogeneous cultural and social contexts, applying this right to regulate AI systems poses significant challenges.

Globally, despite advances in the research to enhance the explainability of AI systems, the hitherto proposed frameworks are still devoid of due considerations for diversity in cultural, social and ethnic fabric of stakeholders. Most of the studies indicate that Western models apply universally; this necessarily does not take into account the non-Western, collectivist societies (Peters & Carman, 2024). Existing frameworks also incorporate transparency at the cost of political and economic ideologies on the explainability of AI systems. As a result, such systems are culturally biased and may lead to inconsistencies, if used globally (Prabhakaran et al., 2022). Globally relevant and harmonized AI regulations must embody the core principles of transparency, accountability, security and dynamic societal adaption (Bhatt, 2025).

Culturally adaptive and stakeholder-sensitive AI systems are the need of the hour. AI regulating frameworks must consider cultural, socio-political, ethical and legal heterogeneity across different regions. To ensure equitable and purposeful AI explanations, we need to shift our focus to development of culturally adaptive and stakeholder-sensitive 'Explainable AI' (XAI) models. The 'PEEC Doctrine' propounded by Bhatt & Bhatt in 2023 (Bhatt & Bhatt, 2023) is one promising idea. This proposal not only integrates universally accepted theories of Public Interest, Environmental Sustainability, Economic Development, and Criminal Law (PEEC) to create a realistic approach to development of XAI, but also focuses on transparency considering the broader social, economic, political and legal impacts of AI decisions. The theory has the potential to address AI explanations by duly considering the 'PEEC' elements to promote sustainability and ease of access to explainability while ensuring sufficient accountability with a multi-dimensional perspective on XAI systems to serve the real-world societal needs.

AI/ XAI systems are complex algorithms blending social, ethical and human values. Human perceptions, values and interpretations are crucial in determining the success of these systems. However, conflicting goals and objectives, dynamic and unpredictable and an unforeseen environment, value-laden issues, and a complex interplay between human values, technology, and societal norms calls for a structured and iterative methodological approach besides purely technological or legal strategy to deal with the issue.

In these contexts, the study aims to investigate 'Right to Explanation' and 'PEEC Doctrine' by duly considering diverse cultures and values of 'G20 Giants' (USA, Germany, Japan, India, Brazil, & Russia) using Soft System Methodology (SSM) to develop Key Performance Indicators (KPIs) for adaptable, transparent and culturally sensitive XAI regulations that would enhance the trust and efficacy of AI systems worldwide.

1. Ethical and Cultural influences on XAI in 'G20 Giants'

Sizeable differences in the cultural and ethical core values across many nations especially in terms of individualism (personal autonomy & self-determination), collectivism (Prioritization of Group Solidarity and Communal Well-being), trust in technology (Confidence in Digital Innovations and Automated Systems) and respect for authority (Adherence to Institutional Hierarchies and Governance Structures) has been highlighted by many recent cross-cultural research (Triandis, 2018; Jan et al., 2024). For instance, the United States and Germany are considered individualistic societies, operationalizing personal autonomy and self-reliance (Triandis, 2018). Conversely, cultures like Japan and India, also known as collectivist cultures, emphasize group well-being and social harmony (Eckhardt, 2002). Research evidence suggests that technological diffusion in developed countries rarely reaches the technology adoption rates of developed countries, largely due to socio-economics and digital literacy constraints (Comin & Hobijn, 2011). These cultural features influence policy decisions, societal behaviors, and international relations.

Deeply ingrained societal norms, historical contexts, and national/regional ideologies and policies form the basis for variance in cultural and ethical values across various countries. Table 1 illustrates how different nations uniquely deal with key cultural dimensions.

Table 1. Exploring Cultural Influences of 'G20 Giants' for XAI Regulations

G20 Giants	Ethical and cultural values influencing XAI regulations					
	Individualism (Personal freedom and self-reliance)	Collectivism (Community First Mind-set)	Emphasis on Societal Benefits (Regulations for shared Prosperity)	Trust in Technology (Acceptance of AI, automation, and digital systems)	Demand for Transparency (Accountability and openness in governance and decision-making)	Respect for Authority (Reverence for leadership and order)
USA	Critical	Minimal	Minimal	Significant	Critical	Low
Germany	Significant	Limited	Limited	Significant	Moderate	Significant
Japan	Moderate	Critical	Critical	Moderate	Limited	Critical
India	Limited	Significant	Significant	Limited	Significant	Moderate
Brazil	Limited	Significant	Significant	Limited	Significant	Limited
Russia	Minimal	Significant	Significant	Limited	Minimal	Critical

These elements profusely influence how XAI regulating policies are framed, which shall promote cross-cultural collaboration for universally relevant XAI regulating models simultaneously. This would also guarantee its strict alignment to corresponding societal expectations and values.

2. Existing Provisions of 'Right to Explanation' across 'G20 Giants'

The 'Right to Explanation' has been brought into sharp focus due to increasing universality of legal and ethical debates on AI systems. Many researchers are of the view that this right of explanations may not always be practical and sufficient (Edwards & Veale, 2018; Taylor, 2023; Doshi-Velez et al., 2017). The developed nations, particularly the EU, have established frameworks to deal with complexities in AI decision-making by way of 'Right to Explanation'. Whereas, the developing world is facing a lot of hurdles including legal and technical intricacies in accommodating 'Right to Explanation' into existing frameworks. The practical implementation of the right remains a challenge for developed countries. While a statutory 'Right to Explanation' is a potent mechanism empowering an individual to comprehend and challenge automated systems, its effectiveness depends upon establishing complementary mechanisms like impact assessment and judicial review. To safeguard potential biases and discrimination in automated decision-making, some EU member states have incorporated mandatory impact assessment into their national legislation (Malgieri, 2019). Judicial review provides an additional layer of control and accountability and ensures fairness in automated decision-making (Gacutan & Selvadurai, 2020; Malgieri, 2019).

The complexities of machine language limit the ability of AI developers and operators to provide meaningful and comprehensible explanations for laymen. This calls for a balanced approach whereby neither excessive control nor non-interference circumvents the development of AI systems. Use of AI systems for sectors such as public administration and healthcare ought to meet the standards of safety, transparency and accountability in diverse socio-technical and legal contexts.

Table 2 provides comprehensive information on 'G20 Giants' having provisions of 'Right to Explanation' and corresponding sectors where XAI are currently being employed or planned to be employed.

Table 2. Existing legal provisions of 'Right to Explanation' in 'G20 Giants' for AI systems

Country	Right to Explanation	Existing Legal Provisions	Sector-Specific XAI Example
USA	No explicit legal 'Right to Explanation', but implied in existing laws like the Algorithmic Accountability Act (2022)	– The National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF), 2023[1]. – Federal Trade Commission enacted five law enforcement actions (2024) against operations that use AI hype or sell AI technology that can be used in deceptive and unfair ways[2]	**Finance Sector:** The U.S. Securities and Exchange Commission (SEC) has mandated (2023) that financial institutions must adopt robust AI governance frameworks that emphasize transparency, risk management, and ethical decision-making[3]
Germany	The General Data Protection Regulation (GDPR), 2018 explicitly states that the users have the right to meaningful explanations in automated decision-making	GDPR Article 22, Recital 71, and Article 13, 14 & 15 allows individuals to understand and challenge AI decisions[4]	**Healthcare Sector:** In Germany, under the GDPR, the hospitals are mandated to explain to patient's automated decisions relating to treatment plans and logic behind recommended treatment
Japan	No specific 'Right to Explanation', but for promoting transparency and accountability in use of personal data the Act on the Protection of Personal Information (APPI) exists	A combination of regulations and guidelines is in place[5]. Social Principles of Human-Centric AI (2019), AI Guidelines for Business (2024), and the Japanese Society for Artificial Intelligence (JSAI) Guidelines (2024) attempt to ensure AI development aligns with societal and ethical values	**Automotive Sector:** Autonomously AI-driven vehicles are regulated with strict requirements of safety explainability (Irwan & Mursyid, 2025), but it does not adequately take care of consumers' rights
India	No explicit legal right to explanation, but Personal Data Protection Bill (2023) proposes AI transparency norms	The Personal Data Protection Bill (2023)[6] and the NITI Aayog's (2023)[7] AI policy reinforces explainability and ensures that AI systems are transparent, accountable, and trustworthy	**Banking Sector:** The Reserve Bank of India is working on developing a 'Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI)' in the Financial Sector[8]

1 National Institute of Standards and Technology (NIST). AI Risk Management Framework. https://clck.ru/3QmQ64

2 Federal Trade Commission. (2024). FTC announces crackdown on deceptive AI claims and schemes. Federal Trade Commission. https://clck.ru/3QmQ9Z

3 Essert. AI Governance Frameworks for Financial Institutions. https://clck.ru/3QmQAn

4 General Data Protection Regulation (GDPR). https://clck.ru/3QmQCt

5 Habuka, H. (2023). Japan's approach to AI Regulation and its impact on the 2023 G7 Presidency. Center for Strategic & International Studies. https://clck.ru/3QmQYX

6 Ministry of Law and Justice. (2023). Digital Personal Data Protection Act, 2023. The Gazette of India, CG-DL-E-12082023-248045. https://goo.su/m3v3Zp

7 NITI Aayog. (2023). National Strategy for Artificial Intelligence. NITI Aayog. https://goo.su/nfPaH

8 Reserve Bank of India. (2023). RBI mandates explainability in AI-driven loan approvals. Reserve Bank of India. https://goo.su/SWi8E

Country	Right to Explanation	Existing Legal Provisions	Sector-Specific XAI Example
Brazil	Proposed explicit 'Right to Explanation' vide Bill 2383/2023[9]	The proposed senate approved Bill guarantees that the individuals or groups affected by high risk AI shall have a right to timely and understandable explanation of the decisions, recommendations and/or predictions made using AI systems. The proposed bill[10] establishes a national regulatory framework governing the use and development of AI systems in Brazil	**Public Safety Sector**: AI systems are employed to predict and prevent crime in major cities of Brazil (Ribeiro et al.,2024)
Russia	No explicit 'Right to Explanation', though the principles outlined in Russia's AI strategy focus on having AI systems that are responsibly designed to protect individuals' rights with transparency	Russia's National AI Development Strategy aims to generate Russia-developed AI products and Services. The emphasis is on development of 'Strong AI' for military operations and national developments[11]	**Military Sector:** Use of AI to provide data analysis for better and faster decision-making capacity to the warfighter in the battlespace[12]

3. Assessing Applicability of 'PEEC' Doctrine for XAI in 'G20 Giants'

A qualitative assessment of the 'PEEC' framework proposed by Bhatt & Bhatt, 2023 is imperative to validate the diverse approaches to AI regulations and context-specific policies that reflect each country's unique socio-cultural and political landscape. AI regulating policies across countries are shaped by their respective socio-cultural priorities and governance ideologies. The elements of 'PEEC' framework, viz. public interest, environmental sustainability, economic development and criminal law have to be evaluated accordingly.

Public interest focuses differ from country to country. The United States prioritizes consumer protection and Germany emphasizes privacy of data, while countries like India and Japan are more inclined to social harmony and equitable access. Countries like Brazil and Russia intend to address governance failures and ensure state security. When it comes to environmental sustainability, countries like the United States and Germany aim to leverage AI for private sector innovation and improving industrial productivity and efficiency. Japan and India are more inclined to achieve long-term goals in smart city planning and water management. Both Brazil and Russia understand that AI systems can

9 Data Privacy Brazil Research Association. (2024). The artificial intelligence legislation in Brazil: Technical analysis of the text to be voted on in the Federal Senate plenary. https://clck.ru/3QmR23

10 The Mattos Filho News Portal. (2024). Framework for artificial intelligence in the Senate. https://goo.su/lbFTrr

11 CNA. (2020). Artificial intelligence in Russia: Issue 11. https://clck.ru/3QmRSw

12 Boulanin, V., & Zerbo, L. (2023, July 20). Roles and implications of AI in the Russian-Ukrainian conflict. Russia Matters. https://clck.ru/3QmRTy

help attain environmental sustainability. Brazil focuses on combating climatic issues while the Russian approach is more focused on the energy sector.

Economically, Russia and Brazil thrive to drive state-led innovations and technological upgradations, while the United States and Germany endorse innovation with structured labour protection and concerns. Japan and India are both keen on developing robotics and finance technologies. AI use for criminal laws also varies significantly. While the United States balances security and personal liberty, Germany emphasizes oversight. Japan employs AI with checks and balances, the Indian approach is to develop safeguards. The Brazilian approach is all about tackling whereas Russia prioritizes security through surveillance. This diverse set of considerations highlights the intricate interplay that ought to be considered for XAI development worldwide.

It is worthwhile assessing the fitness of 'PEEC' principles as proposed by Bhatt & Bhatt, 2023 for ensuring that the XAI regulations shall remain effective, contextual and aligned with societal expectations worldwide. Table 3 shows the fitness of 'PEEC' principles for development of XAI across 'key G20 economies'.

Table 3. Heat-map of Fitness of 'PEEC' Principles across countries for XAI development

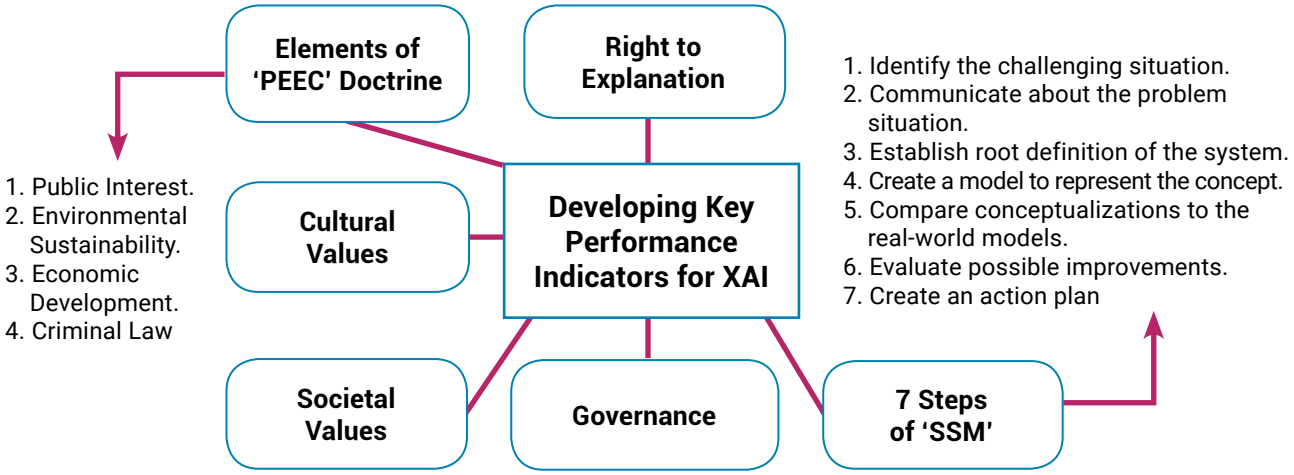
No.	PEEC' Principle	USA	Germany	Japan	India	Brazil	Russia
1	Transparency & Accountability	Yes	Yes	No	Yes	Yes	No
2	Data Security & Privacy	Yes	Yes	No	Partial	Partial	No
3	Ethical Considerations	Yes	Yes	Partial	Yes	Yes	Partial
4	Environmental Impact Assessment	Partial	Yes	Yes	Yes	Yes	No
5	Economic Incentives & Innovation	Yes	Yes	Yes	Yes	Yes	Yes
6	Risk Management & Liability	Partial	Yes	No	Partial	Partial	Yes
7	Public Participation & Consultation	Yes	Yes	No	Yes	Yes	No
8	Law Enforcement & Criminal AI Regulation	Partial	Yes	No	Partial	Partial	Partial
9	Interdisciplinary Collaboration	Yes	Yes	Partial	Yes	Yes	No

4. Developing Integrated Key Performance Indicators (KPIs) for XAI

A purely technical or quantitative approach cannot entirely cover all the inherent complexity, subjectivity, and ethical dimensions of the XAI regulating framework. To forge a truly comprehensive and robust framework, it is imperative to actively engage and incorporate the diverse perspectives of all stakeholders involved in AI systems. Soft systems methodology (SSM) is one interesting approach for tackling problematic and messy situations of diverse varieties, particularly those involving human systems (Checkland & Poulter, 2020).

The SSM allows users to deal with complex technical, political and socio-cultural problems in an organized manner and forces them to look for a holistic solution. The integration of 'PEEC' principles and 'SSM' can provide a potent tool for development of integrated KPIs for practical policy regulations on XAIs.

To truly tap the intricacies of the explainability of AI systems, one must look beyond just the technicalities involved. The authors proposes a novel approach of developing a comprehensive 'Key Performance Indicators' (KPIs) that would bring on board due considerations of Public Interest, Environmental Sustainability, Economic Development, Criminal Law through the structured procedure of 'Soft System Methodology' for a holistic assessment of AI's implications on social, economic, political and legal regimes. Figure shows the conceptual model adopted for the said purpose.



Conceptual Model for Development of KPIs

To develop robust and universally acceptable KPIs for XAI, the SSM approach was employed to incorporate and integrate key dimensions of public interest, environmental sustainability, economic development, legal issues and governance. The structured and iterative process involved in SSM ensured that the developed KPIs would be apt and fitting for diverse cultural and legal contexts. Firstly, a thorough 'Problem Identification' for analysis of challenges to AI's transparency across different landscapes was explored. Secondly, a comprehensive literature review of existing AI policies, academic research publications and news articles were critically analyzed for conducting a 'Rich Picture Analysis' for visually mapping the expectations of key AI stakeholders, viz. policy makers, public, industry and legal experts. Thirdly, for refinement of 'PEEC Dimensions & Impact Areas', 'Root definition' and 'Conceptual Modelling' approach was employed to ensure its alignment with ideologies relating to socio-economic, legal, ethical and environmental sustainability aspects. Fourthly, a 'Comparative Analysis' for validation of real-world

applicability of AI regulation was undertaken. Lastly, an 'Iterative Refinement Cycle' helped ensure that the developed KPIs were not just attuned to the needs but were also practically implementable, rendering streamlined data collection and measurable criteria. Table 4 shows a proposed comprehensive KPI framework for XAI.

For high-risk decisions where the consequences of an unexplained decision are severe, the proposed 'Clarity and Trust Index' (CTI) can be kept at 90 percent to 100 percent depending upon the requirement. CTI value can be as low as 50 percent to 80 percent for routine automated decisions and 70 percent to 90 percent for strategic decisions.

Table 4. Proposed Comprehensive KPI framework for XAI

'PEEC' Dimension & Impact Areas	Proposed KPI	Definition	How to Calculate?
Public Interest: For establishing control over social and legal issues	**Clarity and Trust Index (CTI)**	Percentage of AI decisions that provide clear, understandable explanations to its user	CTI = (E ÷ T) x 100 Where, E = Explained Decision T = Total Decision
Public Interest: For establishing control over social and economic disparity	**Bias Reduction Index (BRI)**	Reduction of Bias in AI decisions across demographics	BRI = 1 - (BB ÷ MB) Where, BB = Baseline Bias = Observed bias in AI decisions (e.g., selection rate disparity between groups). MB = Maximum Bias = The worst-case bias scenario (e.g., one group gets 100%, another gets 0%). If BRI = 0, Maximum Bias = 100, Perfect Fairness
Environmental Sustainability: For ensuring environmental compliance and corresponding green economics	**AI Carbon Footprint Index (AICFI)**	Measurement of environmental impact of AI systems in terms of their energy consumption and greenhouse gas emissions	AICFI = ACF x TD Where, ACF = Energy consumed by the AI system (kWh per decision) X Carbon Emission Factor (kg CO per kWh), which depends on the energy source TD = Total Decision
Economic Development: For ensuring a positive impact of AI on regional culture and economics	**AI Socio-economic Benefit-Cost Ratio (ASEBC)**	Measurement of employment generation, economic benefits and the associated cost of deployment of AI systems to reflect upon the impact of this technology on the economy and culture	ASEBC = EB ÷ CD Where, EB = Economic benefit of deployment of AI system CD = Cost associated for AI deployment
Legal & Governance: For tracking the efficacy of AI systems across different cultures and legal systems	**Cultural & Legal Accountability Score (CLAS)**	Measurement of disputes, public grievances and their corresponding resolutions regarding AI usage across different cultures having their legal regulating mechanism on AI	CLAS = RD ÷ TG Where, RD = Total number of Resolved AI disputes TG = Total number of AI Grievances/ Disputes raised

Ideally, the proposed 'Bias Reduction Index' (BRI) shall be 100 percent, though above 90 percent it shall remain acceptable in most cases. Theoretically, the proposed 'AI Carbon Footprint Index' (AICFI) shall be as low as possible. However, the 'AICFI' can

also be attuned to suit the UN Sustainable Development Goals (SDGs). Most countries would prefer the proposed 'AI Socio-economic Benefit-Cost Ratio' (ASEBC) higher than 1.0 or greater, however, efforts must focus on maximizing net tangible socio-economic benefits. The proposed 'Cultural & Legal Accountability Score' (CLAS) shall ideally be 1.0, though a value higher than 0.9 in most cases would suffice the public expectations. Thorough analysis of country-specific context, stakeholder engagement and necessary understanding of cultural contextual factors shall influence the feasibility and desirability of proposed KPIs indicator values. The onus is on policymakers to devise accurate ranges to reflect national circumstances while remaining globally acceptable in contributing and realizing the true potential of XAI systems for the betterment of mankind.

Effective country-specific careful adjustments to the proposed KPIs will optimize it for universal use. While all the five KPIs are relevant for 'G20 Giants', their relative importance hinges on country-specific socio-cultural-legal contexts. The long-running regulatory debates and corporate initiatives in the USA demand higher 'CTI'. While, in Germany, the provisions of GDPR suggest a need for higher 'BRI' and lower 'AICFI'. Brazilian and Indian policies are more centered on having higher 'CLAS' and 'ASEBC'. Russian policies look to leverage AI in governance and thus have higher 'ASEBC' with a firm strategic focus to uphold national sovereignty and integrity.

Conclusions

Diversities in cultural, ethical, socio-economic and legal choices made by society pose a mammoth challenge before the policy makers to develop a regulating XAI framework that fits international requirements. These factors are in fact, the limiting determinant that have the potential to clinch the success or failure of XAI regulations. Finding a path forward requires attention not only to technological aspects, but most essentially the human dimensions to it. 'Right to Explanation', 'Public Interest', 'Environmental Sustainability', 'Economic Development', and 'Criminal Law' (PEEC) are all exigent and shall ever remain central to all our attempts to regulate AI technologies.

The study proposes a novel KPI based regulating model for XAI based on the principles of PEEC using a structured approach of 'Soft System Methodology'. To truly tap the potential of the proposed KPI model, countries must set nationally relevant indicator ranges that hold value internationally. Besides deracinating the problems of regulating XAI across diverse cultural, ethical and legal landscapes, the proposed model ensures that the XAI regulating framework duly considers the human dimensions as it seeks to harness the true potential of AI. This approach will inspire AI-driven society in the future.

The study only considers the cultural complexities of 'G20 Giants'. Further research or investigations shall encompass a wider spectrum to include other developed and developing nations to make the XAI regulating framework adaptable to diverse national and global demands.

References

Bhatt, N. (2025). Crimes in the Age of Artificial Intelligence: a Hybrid Approach to Liability and Security in the Digital Era. *Journal of Digital Technologies and Law*, *3*(1), 65–88. https://doi.org/10.21202/jdtl.2025.3

Bhatt, N., & Bhatt, J. (2023). Towards a novel eclectic framework for administering artificial intelligence technologies: A proposed 'PEEC' doctrine. *EPRA International Journal of Research and Development (IJRD)*, *8*(9), 27–36. https://doi.org/10.13140/RG.2.2.11434.18888

Checkland, P., & Poulter, J. (2020). Soft Systems Methodology. In M. Reynolds, S. Holwell (Retired) (Eds), *Systems Approaches to Making Change: A Practical Guide* (pp. 201–253). Springer, London. https://doi.org/10.1007/978-1-4471-7472-1_5

Comin, D., & Hobijn, B. (2011). An exploration of technology diffusion. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1116606

Doshi-Velez, F., Kortz, M., Budish, R., Bavitz, C., Gershman, S., O'Brien, D., Schieber, S., Waldo, J., Weinberger, D., Weller, A., & Wood, A. (2017). Accountability of AI Under the Law: The Role of Explanation. *ArXiv*, abs/1711.01134. https://doi.org/10.2139/SSRN.3064761

Eckhardt, G. (2002). Culture's Consequences: Comparing Values, Behaviors, Institutions and Organisations Across Nations. *Australian Journal of Management*, *27*(1), 89–94. https://doi.org/10.1177/031289620202700105

Edwards, L., & Veale, M. (2018). Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"? *IEEE Security & Privacy*, *16*, 46–54. https://doi.org/10.1109/MSP.2018.2701152b

Gacutan, J., & Selvadurai, N. (2020). A statutory right to explanation for decisions generated using artificial intelligence. *International Journal of Law and Information Technology*, *28*(3), 193–216. https://doi.org/10.1093/ijlit/eaaa016

Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018). Explaining Explanations: An Overview of Interpretability of Machine Learning. In *2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA)*, Turin, Italy, 2018 (pp. 80–89). https://doi.org/10.1109/DSAA.2018.00018

Hacker, P., Krestel, R., Grundmann, S., & Naumann, F. (2020). Explainable AI under contract and tort law: Legal incentives and technical challenges. *Artificial Intelligence and Law*, *28*(4), 415–439. https://doi.org/10.1007/s10506-020-09260-6

Irwan, M., & Mursyid, M. (2025). AI-Driven Traffic Accidents: A Comparative Legal Study. *Artes Libres Law and Social Journal*, *1*(1), 1–20. https://doi.org/10.12345/jxt3j717

Jan, J., Alshare, K. A., & Lane, P. L. (2024). Hofstede's cultural dimensions in technology acceptance models: a meta-analysis. *Universal Access in the Information Society*, *23*(2), 717–741. https://doi.org/10.1007/s10209-022-00930-7

Malgieri, G. (2019). Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations. *Computer Law & Security Review*, *35*(5), 105327. https://doi.org/10.1016/J.CLSR.2019.05.002

Peters, U., & Carman, M. (2024). Cultural bias in explainable AI research: A systematic analysis. *Journal of Artificial Intelligence Research*, *79*, 971–1000. https://doi.org/10.1613/jair.1.14888

Prabhakaran, V., Qadri, R., & Hutchinson, B. (2022). Cultural incongruencies in artificial intelligence. *arXiv preprint arXiv:2211.13069*. https://doi.org/10.48550/arXiv.2211.13069

Ribeiro, L. H. da C., Silva, C. M. da, & Viana, P. W. P. (2024). Artificial intelligence as a tool for predicting crime in large Brazilian cities. *Revista FT*, 28. https://doi.org/10.5281/zenodo.11100354

Taylor, E. (2023). Explanation and the Right to Explanation. *Journal of the American Philosophical Association*, *10*(3), 467–482. https://doi.org/10.1017/apa.2023.7

Triandis, H. C. (2018). *Individualism and collectivism*. Routledge. https://doi.org/10.4324/9780429499845

Authors information

Neelkanth Bhatt – PhD, Head of the Department & Associate Professor, Department of Civil Engineering, Government Engineering College
Address: Near Mavdi-Kankot Road, Rajkot, Pin Code 360 005, Gujarat, India
E-mail: neelkanth78bhatt@gmail.com
ORCID ID: https://orcid.org/0000-0003-0315-2985
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58919442100
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KRO-8652-2024
Google Scholar ID: https://scholar.google.com/citations?user=L7K-e3IAAAAJ

Jaikishen Nathalal Bhatt – Bachelor of Commerce, Retired Social Security Officer, Employees' State Insurance Corporation
Address: Panchdeep Bhavan, Ashram Road, Ahmedabad, Pin 380 009, Gujarat, India
E-mail: neelkanth.bhatt@gujgov.edu.in
ORCID ID: https://orcid.org/0009-0000-3645-829X

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – July 18, 2025
Date of approval – August 2, 2025
Date of acceptance – December 20, 2025
Date of online placement – December 25, 2025

Научная статья
УДК 34:004:340.1:004.8:004.051
EDN: https://elibrary.ru/uiujcv
DOI: https://doi.org/10.21202/jdtl.2025.26

Объяснимый искусственный интеллект и правовые традиции: разработка универсальных ключевых показателей эффективности для стран «Большой двадцатки»

Нилкант Бхатт ✉

Государственный инженерный колледж, Раджкот, Индия

Джайкишен Наталал Бхатт

Государственная корпорация страхования работников, Ахмедабад, Индия

Ключевые слова

искусственный интеллект,
общественные интересы,
объяснимый искусственный интеллект,
право,
прозрачность алгоритмов,
уголовное правосудие,
цифровые технологии,
экологическая устойчивость,
экономическое развитие,
этика

Аннотация

Цель: изучить концепцию «право на объяснение» в контексте доктрины PEEC (общественные интересы, экологическая устойчивость, экономическое развитие, уголовное правосудие) для разработки ключевых показателей эффективности, отражающих социокультурные особенности различных стран и обеспечивающих адаптивность, прозрачность и культурную релевантность в регулировании объяснимого искусственного интеллекта.

Методы: в исследовании применяется уникальный методологический подход, сочетающий итеративные процессы методологии мягких систем с теоретической базой, основанной на принципах PEEC. Подобная интеграция позволяет комплексно рассмотреть социальные, экономические, политические и правовые режимы крупнейших стран «Большой двадцатки»: Соединенных Штатов Америки, Федеративной Республики Германия, Японии, Республики Индия, Федеративной Республики Бразилия и Российской Федерации – при конструировании ключевых показателей эффективности. Предложенные ключевые показатели эффективности применимы для оценки прозрачности и подотчетности систем искусственного интеллекта, упрощая сбор данных и практическую имплементацию в различных культурных контекстах. Разработанная модель соответствует реальным общественным потребностям в принятии решений с использованием технологий искусственного интеллекта.

Результаты: в исследовании предлагается новая правовая модель регулирования объяснимого искусственного интеллекта, основанная на системе ключевых показателей эффективности. Помимо устранения

✉ Корреспондирующий автор

проблем регулирования объяснимого искусственного интеллекта в различных культурных, этических и правовых областях, данная модель гарантирует, что система регулирования объяснимого искусственного интеллекта должным образом учитывает антропоцентрические аспекты, поскольку ориентирована на раскрытие истинного потенциала искусственного интеллекта. Предложенный подход способствует максимально эффективному использованию технологий искусственного интеллекта на благо общества в перспективе устойчивого развития.

Научная новизна: в работе применен уникальный научный подход, учитывающий культурные, этические, социально-экономические и правовые различия при разработке правовой базы для регулирования объяснимого искусственного интеллекта, что позволяет адаптировать ее к различным национальным условиям, одновременно способствуя ответственному управлению искусственным интеллектом с системой сдержек и противовесов.

Практическая значимость: полученные результаты позволяют использовать предложенную правовую модель в практической деятельности государственных органов и разработчиков систем искусственного интеллекта для обеспечения прозрачности и объяснимости технологий. Эффективная корректировка предлагаемых ключевых показателей эффективности с учетом специфики конкретных государств позволит оптимизировать их для универсального применения. Хотя все пять ключевых показателей эффективности актуальны для крупнейших стран «Большой двадцатки», их относительная значимость зависит от социокультурных и правовых условий конкретного государства. Дальнейшие исследования должны охватывать более широкий спектр вопросов, включая другие развитые и развивающиеся страны, для адаптации регулирования объяснимого искусственного интеллекта к различным национальным и глобальным требованиям.

Для цитирования

Бхатт, Н., Бхатт, Дж. Н. (2025). Объяснимый искусственный интеллект и правовые традиции: разработка универсальных ключевых показателей эффективности для стран «Большой двадцатки». *Journal of Digital Technologies and Law*, *3*(4), 660–676. https://doi.org/10.21202/jdtl.2025.26

Список литературы

Bhatt, N. (2025). Crimes in the Age of Artificial Intelligence: a Hybrid Approach to Liability and Security in the Digital Era. *Journal of Digital Technologies and Law*, *3*(1), 65–88. https://doi.org/10.21202/jdtl.2025.3

Bhatt, N., & Bhatt, J. (2023). Towards a novel eclectic framework for administering artificial intelligence technologies: A proposed 'PEEC' doctrine. *EPRA International Journal of Research and Development (IJRD)*, *8*(9), 27–36. https://doi.org/10.13140/RG.2.2.11434.18888

Checkland, P., & Poulter, J. (2020). Soft Systems Methodology. In M. Reynolds, S. Holwell (Retired) (Eds), *Systems Approaches to Making Change: A Practical Guide* (pp. 201–253). Springer, London. https://doi.org/10.1007/978-1-4471-7472-1_5

Comin, D., & Hobijn, B. (2011). An exploration of technology diffusion. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1116606

Doshi-Velez, F., Kortz, M., Budish, R., Bavitz, C., Gershman, S., O'Brien, D., Schieber, S., Waldo, J., Weinberger, D., Weller, A., & Wood, A. (2017). Accountability of AI Under the Law: The Role of Explanation. *ArXiv*, abs/1711.01134. https://doi.org/10.2139/SSRN.3064761

Eckhardt, G. (2002). Culture's Consequences: Comparing Values, Behaviors, Institutions and Organisations Across Nations. *Australian Journal of Management*, *27*(1), 89–94. https://doi.org/10.1177/031289620202700105

Edwards, L., & Veale, M. (2018). Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"? *IEEE Security & Privacy*, *16*, 46–54. https://doi.org/10.1109/MSP.2018.2701152b

Gacutan, J., & Selvadurai, N. (2020). A statutory right to explanation for decisions generated using artificial intelligence. *International Journal of Law and Information Technology*, *28*(3), 193–216. https://doi.org/10.1093/ijlit/eaaa016

Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018). Explaining Explanations: An Overview of Interpretability of Machine Learning. In *2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA)*, Turin, Italy, 2018 (pp. 80–89). https://doi.org/10.1109/DSAA.2018.00018

Hacker, P., Krestel, R., Grundmann, S., & Naumann, F. (2020). Explainable AI under contract and tort law: Legal incentives and technical challenges. *Artificial Intelligence and Law*, *28*(4), 415–439. https://doi.org/10.1007/s10506-020-09260-6

Irwan, M., & Mursyid, M. (2025). AI-Driven Traffic Accidents: A Comparative Legal Study. *Artes Libres Law and Social Journal*, *1*(1), 1–20. https://doi.org/10.12345/jxt3j717

Jan, J., Alshare, K. A., & Lane, P. L. (2024). Hofstede's cultural dimensions in technology acceptance models: a meta-analysis. *Universal Access in the Information Society*, *23*(2), 717–741. https://doi.org/10.1007/s10209-022-00930-7

Malgieri, G. (2019). Automated decision-making in the EU Member States: The right to explanation and other «suitable safeguards» in the national legislations. *Computer Law & Security Review*, *35*(5), 105327. https://doi.org/10.1016/J.CLSR.2019.05.002

Peters, U., & Carman, M. (2024). Cultural bias in explainable AI research: A systematic analysis. *Journal of Artificial Intelligence Research*, *79*, 971–1000. https://doi.org/10.1613/jair.1.14888

Prabhakaran, V., Qadri, R., & Hutchinson, B. (2022). Cultural incongruencies in artificial intelligence. *arXiv preprint arXiv:2211.13069*. https://doi.org/10.48550/arXiv.2211.13069

Ribeiro, L. H. da C., Silva, C. M. da, & Viana, P. W. P. (2024). Artificial intelligence as a tool for predicting crime in large Brazilian cities. *Revista FT*, 28. https://doi.org/10.5281/zenodo.11100354

Taylor, E. (2023). Explanation and the Right to Explanation. *Journal of the American Philosophical Association*, *10*(3), 467–482. https://doi.org/10.1017/apa.2023.7

Triandis, H. C. (2018). *Individualism and collectivism*. Routledge. https://doi.org/10.4324/9780429499845

Сведения об авторах

Бхатт Нилкант – PhD, доцент, заведующий кафедрой гражданского строительства, Государственный инженерный колледж
Адрес: 360 005, Индия, штат Гуджарат, г. Раджкот, ул. Мавди-Канкот
E-mail: neelkanth78bhatt@gmail.com
ORCID ID: https://orcid.org/0000-0003-0315-2985
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58919442100
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KRO-8652-2024
Google Scholar ID: https://scholar.google.com/citations?user=L7K-e3IAAAAJ

Бхатт Джайкишен Наталал – бакалавр коммерции, сотрудник службы социального обеспечения в отставке, Государственная корпорация страхования работников
Адрес: 380 009, Индия, штат Гуджарат, г. Ахмедабад, ул. Ашрам, Панчдип Бхаван
E-mail: neelkanth.bhatt@gujgov.edu.in
ORCID ID: https://orcid.org/0009-0000-3645-829X

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 18 июля 2025 г.
Дата одобрения после рецензирования – 2 августа 2025 г.
Дата принятия к опубликованию – 20 декабря 2025 г.
Дата онлайн-размещения – 25 декабря 2025 г.

Research article
UDC 34:004:340.1:004.8:808.1:347.779
EDN: https://elibrary.ru/burdtt
DOI: https://doi.org/10.21202/jdtl.2025.27

Ethical Implications of Using Artificial Intelligence in Intellectual Property Creation: Authorship, Ownership and Responsibility Issues

Kolawole Afuwape
O. P. Jindal Global University, Sonipat, India

Keywords

algorithmic bias,
artificial intelligence,
copyrighht,
copyright,
digital technology,
ethics,
generative artificial intelligence,
intellectual property,
law,
patent law

Abstract

Objective: to critically assess the ethical issues related to the use of artificial intelligence in the development of intellectual property objects, with an emphasis on the problems of authorship, ownership, originality and responsibility.

Methods: the research uses a comprehensive analysis of the existing regulatory framework and case law in the field of intellectual property and artificial intelligence. A systematic review of the scientific literature includes publications in peer-reviewed scientific journals and analytical reports on the ethical aspects of the use of artificial intelligence, legislation in the field of intellectual property and the transformation of the digital landscape. The author provides a critical synthesis of scientific arguments and theoretical discussions regarding the ethical status of artificial intelligence as an author and co-author of creative works. The study assesses artificial intelligence systems through the prism of fairness, accountability and transparency concepts.

Results: the lack of legal recognition of artificial intelligence as an author or inventor was revealed in most legal systems worldwide; the intellectual property paradigm is still based on human-centered ideas about creativity and invention, which creates a regulatory gap. The study established significant ambiguity in the fields of ownership and accountability, since artificial intelligence, without legal personality, creates an ethical problem: should the intellectual property created by an autonomous system belong to the developer, user, data provider or remain in the public domain. The author identified the risks of bias and

exploitation in creative industries where artificial intelligence is trained using copyrighted materials without permission or compensation to their creators. There has been a shift towards double ethical standards due to jurisdictional and sector differences in relation to works created using artificial intelligence. This promotes unfair global differences in the protection of intellectual property rights.

Scientific novelty: the author presented a multifaceted interdisciplinary analysis that integrates the legal, ethical and technological fields of research on intellectual property created using artificial intelligence. The developed conceptual framework may help to comprehensively solve the ethical and regulatory issues arising in connection with works created with the participation of artificial intelligence, including the justification of the need for legal reform, taking into account the ethical imperatives of modern technological development.

Practical significance: The study contains ethically grounded recommendations for legislators, legal practitioners, and technology developers to amend intellectual property legislation to effectively address issues of authorship, ownership, and accountability in relation to works created using artificial intelligence. The recommendations may ensure a balance between stimulating innovations and protecting the rights of a human author.

For citation

Afuwape, K. (2025). Ethical Implications of Using Artificial Intelligence in Intellectual Property Creation: Authorship, Ownership and Responsibility Issue. *Journal of Digital Technologies and Law, 3*(4), 677–704. https://doi.org/10.21202/jdtl.2025.27

Contents

Introduction

In the last few years, great strides in AI systems and technologies have turned AI into a key pillar of business planning (Aldoseri et al., 2024). Businesses of all industries are embracing AI at a more enthusiastic rate than ever before, all in search of a greater degree of operational efficiency and more informed decision making (Ali et al., 2024). Application, services, and infrastructure spending in the world as it relates to AI is at an all-time high with IDC estimating that the number will rise to USD 632 billion by 2028, which is a compound annual growth rate of 6 percent from 2023 to 2028[1] (Hosting Journalist).

Further development in AI capabilities is creating monumental questions for the applicability of the intellectual property laws on AI and the work it produces (Salle & Rini, 2025). The accelerating evolution of AI is pushing enterprises to create internal architectures that put emphasis on ethical decision making (Olaniyi, 2024). IP is one of the critical and most disruptive subjects in AI governance (Schmit et al., 2023). Under wide recognition, AI has been seen as a very helpful commodity; people look at its challenges and innovative prospects, especially in the case of intellectual property (Ooi et al., 2025).

There is a high rate of adoption of AI, and it seems likely to lead to an even greater scale in commercial use of AI across a wide range of sectors by 2025 (Md et al., 2025). Given IP issues arise with AI, actors applying such technologies must plan proactively to manage the IP ecosystem (Lalanda & Roig, 2025). As AI law is being authored, businesses must strive to remain compliant with copyright standards whilst at the same

[1] Global AI Infrastructure Spending to Double by 2028, Reaching $632B. Hosting Journalist. https://clck.ru/3Qd7xh

reinforcing their own proprietary asset protection (Gaffar & Albarashdi, 2025). To become shapers of successful strategies in an AI economy, companies must understand how current laws impact ai development and stay current with the continuing legal landscape (Shalaby, 2024).

Technology is a key and imperative variable that shapes the present state of innovation (Vărzaru & Bocean, 2024). The role played by modern technology in terms of development is as critical as can be, but it has brought down the need for human intervention almost completely – or in some cases, altogether, in some cases. This creates a distinctive challenge: comparing works created by software and algorithms with those produced indicative of human effort only. In today's commercial world where IP rights ownership becomes a determining factor of the prospects of company expansion, this problem is quite a significant challenge (Mary & Enoch, 2024). The argument over whether entities from the non-human world such as software and algorithms deserve rights is an issue on the lips of discussion around intellectual property (Tunç, 2025).

1. Who owns AI-generated intellectual property?

The conflict between technology and copyright has gone through the initial creation of the printing press as well as the advancements towards creation of digital media and the internet (Iguh & Anyanor, 2023). With each innovation in technology, there has been a need to change copyright regulations (Kumar, 2024). Berne convention according to Article 2 only allows human creation to enjoy copyright (Al Da'jeh & Alzubi, 2024). If an AI creates content, whose rights should be claimed – of the AI developer or of the user who launched the process? Policy makers must revise the law to address these challenges. Though there is common understanding that human's creativity is needed for copyright, the development of AI-generated works has complicated this practice (Hutson, 2024).

As recognized by notable experts on copyright, a key international agreement, the Berne Convention lays particular emphasis on focusing on human creativity in the world of copyrights (Geiger, 2024). Article 2 of the Berne Convention says that between its nations the word "author" would mean those who physically produce the works, which effectively does away with need to have an explicit definition of authorship (Olwan& Al-Balushi, 2023). Although the Convention permits a "maker" to protect copyright in cinematographic works, it is underscoring a growing number of AI-created works test copyright systems' inequities towards the rights of human authors (Singh, 2024).

A lot of discussion is stirred up around the possibility of copyrighting AI generated work and the necessity for legal amenities to acknowledge the influence of AI in the creation process. The regulatory climate describes the controversy around GenAI's training data

being in violation of copyright protections, as well as specifies who is held responsible for doing so – the service provider or the user (de la Durantaye, 2025). In such conversations, the disparity between the forward momentum technology and desire to maintain copyright norms becomes apparent. Some areas such as the EU and the US allow more freedom to innovate, except in the cases of text and data mining exemptions, and fair use doctrine but with extra thorns and obstacles to overcome (Margoni & Kretschmer, 2022). Adjustment of IP protection requirements should be considered under different international regions as AI technologies are already largely applied globally (Marchenko et al., 2024). There are government practices such as the DMCA and others that provide protection and exceptions, but the complex use of GenAI makes the old ways of achieving protection complex (Chesterman, 2025).

The perspective of inventing has changed with the increasing speed of AI development and increased ability of data processing, pattern recognition, and predictive functions to innovation-oriented areas (Chen et al., 2024). The results provided by contemporary AI systems require a minimum or non-existence of human input. Patent for these creations can be issued, if the creator is a human. Patents conventionally require a human inventor at their heart (Ajani, 2020). The basis of patent law is to encourage the inventors by rewarding them for their revolutionary contributions. Copyright safeguards legally speak to intelligent original inventions, not simply new results or simple upgrades of pre-existing concepts (Tan, 2024). The concept of 'invention' as an idea includes the 'unique intellectual thought uniquely originated by the inventor, as the fundamental mental labour in inventive creation (Knutson, 2020).

The previous consensus is that AI systems are without legal capacity or personality and therefore cannot be baked with IP rights (Aveni & Faria, 2024). There is a wide difference of ideas regarding who the IP right owner is and if there must be an appointed rights owner (Contreras, 2022). The owner of an AI system may also potentially have an ownership interest in an AI generated invention or work (Lopez & Gonzalez, 2024). Ownership could be vested in the author of the code for the AI system; the next one to control the system (Padmanabhan & Wadsworth, 2024). The end user or steward of AI (Kelly et al., 2023); or a collective of these participants. Ownership of IP may also be assigned, through contract language (Srivastava, 2024).

2. How does AI challenge existing copyright and patent laws?

Through IP laws, the owners of intellectual property can secure themselves by prohibiting other people from taking unconventional advantage of their work (Castaldi et al., 2024). It is for patent owners to deny others the use of inventions without proof of authorization

while copyright owners can prevent people from reproducing their creative works without approval[2] (The World Trade Organization). With such protection in place, IP owners can instead gain recognition as well as financial reward for their creations, now underpinning their efforts to put more resources and attention into their artistic work.

Undoubtedly, the logic behind this is the key driver of the establishment and the performance of the IP legislation. Contrary to such, AI systems are not interested in such incentives because they do not derive their functions from external motivators (Ai et al., 2022). Therefore, it would not be unreasonable to ask: are AI systems under the same IP laws as human creations were? The present analysis will, for the most part, focus on how AI challenges the effective functioning of patent and copyright legislation.

3. What are the ethical concerns surrounding plagiarism, bias, and accountability in AI-created works?

AI content generators generated concerns on matters like bias, plagiarism, copyright violators, misuse, production of misinformation, fake news and deceptive information (Ghiurău & Popescu, 2024). These risks can lead to tarnished reputation; widespread proliferation of deceiving content; and increased threat of provoking violence. The increased risk of biased answers is one of the most burning ethical problems connected with the use of AI in text generation, especially with platforms such as ChatGPT (Kim, 2024). Because content generators' large language models are also trained on vast amounts of information, images, and web data, their biases are likely to crop up in the generated text (Tyagi, 2024). By extension, such biased responses might erode outputs and fairness' accuracy and promote discriminatory inclinations such as those based on race or even gender (Varona & Suárez., 2022).

The prejudice contained in contents produced by AI is not a characteristic of technology but a process of development and training (Ferrara, 2023). By taking LLMs through biased information and data, consciously or subconsciously, the output which the model produces will also reflect that bias (Tiwari, 2025). To prevent the occurrence of biased end results, delivery of fairness is also necessary and therefore it becomes very important to use an unbiased, diverse, and representative dataset to obtain fairness. Despite its promises and far-reaching reputation, as well as being much advertised, Generative Artificial Intelligence is not free from its flaws (Haase & Hanel, 2023). ChatGPT and other chatbots have been seen to be unreliable, sometimes misinformed, and unsound in answers, forcing some users to question its accuracy (Xiong, 2024). In addition, developers and users, and regulators

[2] The World Trade Organization, Part II – Standards concerning the availability, scope and use of Intellectual Property Rights. https://clck.ru/3Qd8Aa

need immediate attention to the ethical issues posed by AI generators of content such as issues regarding authenticity, bias, and exploitation (Uddagiri & Isunuri, 2024). Otherwise, we may face unaccounted for and harmful consequences to society, to businesses, and to the economy.

One of the major ethical concerns is the danger that AI content generators can be used to malicious ends. ChatGPT and other text-generators pose threats because they also can be abused to create content that can be used for harmful purposes, including the spreading of propaganda or hate speech or spreading false or misleading reports.

Such tools, such as ChatGPT, increase the rate of plagiarism by authors and students, and it is hard to discover the instances (Khalaf, 2025). To deal with plagiarism involving AI tools, new approaches, such as ChatZero and AI Text Classifier, which can distinguish AI and human writings, have been proposed (Elkhatat et al., 2023).

There is a threat that hackers will hack AI-generated content tools to write personalized deceiving spam emails and stealthy graphic messages (Arif et al., 2024). Consequently, cyber threats could be brought in large numbers of people, possibly injuring many users (Afaq et al., 2023). Chatbot platforms obtained private personal data from users meaning that third parties may contaminate, retain or judge the data (Giordani, 2024).

Development of AI capabilities brings heavy weight upon the manufactures of AI and regulators because of uncertainty regarding who owns the copyright when the content is generated by AI (Peukert & Windisch, 2024). GenAI models are incredibly dependent on a tremendous volume of unpaid and uncompacted data uploaded by humans that is often accompanied by an abhorrence of pertinent regulations (Huang et al, 2024). The application of such techniques usually involves argumentation over ethics and law, as, as a rule, such material is taken without authorization and then incorporated into the training data (Gorwa et al., 2020). The rapid rollout and global proliferation of Gen AI technologies such as ChatGPT have discomfited established legal and ethical ground rules across the globe and caused disruption within the information supply chain and proliferation of Deepfakes. Governments need to pass regulations to enhance GenAI development by supporting the current industry and promoting its growth.

4. Recommendations for addressing Ethical Concerns

Content platforms require distinct rules and controls to represent AI use in a sensible manner (Marsoof et al., 2022). The frameworks developed respond to privacy and bias issues while allowing a code of ethics to govern the conduct of content creators using AI. Collaborative legal agencies and preeminent organizations enforce the boundaries of ethicality for AI-content creators (Pokrovskaya, 2025).

Users need to identify the weaknesses inherent in providing personal/ confidential information to artificial intelligence platforms (Zhang et al., 2022). People participating

in AI platforms should be aware of both the limitations of such tools and the role of the content creators themselves in forming them (Prakash & Sabharwal, 2024). And it is also important for the users to examine the prompts and ensure the source of the data provided is verifiable but also edit the content where necessary before furthering (Wang et al., 2024). Users should first review and reset the system's results before applying them.

5. AI and the Challenge of Authorship and Ownership

At present, the debate on the control over AI-generated works is at the core of AI-copyright discussion (Werzansky-Orland, 2024). The human creativity in AI-generated products is not enough to emit copyright protection (Oda, 2023). The topic of the identification of AI creators and the related legal issues is a focal point of research on AI and copyright in the present (Chesterman, 2025). On this subject, scholars engage in a debate that involves the perspective that AI-generated works are not sufficiently creative to deserve copyright protection. In this discussion the complexities of AI and copyright in the digital age are demonstrated through the fragmented discourse on copyright issues (Vebritha, 2024).

5.1. Traditional IP frameworks and the requirement of human authorship

It goes without stating that what is inarguably the largest step forward in terms of artificial intelligence lies in its ability to create a creative piece or write (Brandenburg et al., 2025). This is a major threat to the conventional copyrights that were implemented exclusively by human authors. The current structure for IP belonging and protection is largely applied to human authors and does not incorporate contribution from non-human sources (Rotolo, 2025).

The growing prominence of the use of AI technology presents a strong challenge to the endeavors to adjust the existing intellectual property laws to AI technology (Unnikrishnan, 2024). In this case there is a significant amount of obfuscation regarding what rights and responsibilities designers and users of AI systems should follow. At some point, the instructions from the government were necessary to solve the resulting uncertainty.

Intellectual property law's key issue focuses on protecting the rights of people who are generators of various forms of literary and artistic and musical work (Obianyo, 2025). The bulk of these rights revolve around the concept of authorship, which is associated with humanity. As for the Berne Convention, the central agreement for copyright and protection of intellectual property is awarded based on the authorship, that assumes that the creators are human (Xiao, 2023).

Today, the existing rules and protection of AI-produced content are not open to clear specifications on ownership. The framework created by existing laws is based in 'human authorship', which results in partial or not-readily available legal protection to AI content in some scenarios. There is a lot of divergence in legal definitions among countries that run from progressive nations that adopt innovation to traditional domains of Human Centricity.

5.2. Ownership by the AI System

One such radical suggestion is to take the idea that AI should be legally entitled to any products it makes further (Hacker, 2023). It is also receiving skepticism for reasons ranging from legal to philosophical realms. The law now only recognizes ownership in legals persons, which AI systems cannot be eligible for. And it is for this reason that it is so important to provide an AI with legal personhood, as such change will radically change legal systems in the aspect of responsibility and liability already now (Lovell, 2023).

5.3. Ownership by the AI Developer

One way that is possible is to pass on the ownership rights of the AI system to the creator or even the group in charge of the development of the system (Tully, 2024). Under this framework, the developer is identified as the main innovator since it is he/she that develops the algorithm as well as guiding the training of the system. This scenario becomes problematic if the user enters some data or uses the AI in such a way as to significantly influence other outputs the system itself did not anticipate.

5.4. Ownership by the User

The second less radical model is the user who engages AI in the production of content, particularly as a user may add their own information during the use of the AI, such as text instructions relating to emphasis and highlighting (Walter, 2024). Yet, questions remain about the input level of humanity for someone to qualify as the proprietor of any given piece.

5.5. Joint Ownership

Another deficiency could be resolved using joint ownership - the ownership resides with the developer and the user (Padmanabhan & Wadsworth, 2024). It places an agency in both agents and can have some issues included in its execution, for instance, with regards to topics like use of the generated content or potential sale of it.

5.6. No Ownership

Lawyers made by AI suggest that it should be thought of as a public domain rather than subject to the law of copyright (Lemley, 2024). This solves the ownership issue but in the long run it may inhibit people from using Artificial Intelligence and Machine, learning technologies and developing creative ideas.

6. AI-generated work and the legal vacuum

It goes without saying, there are tremendous legal conundrums when addressing questions of ownership regarding works made by artificial intelligence (Chaudhary, 2022). Contemporary intellectual property laws delineate the right of authors or copyright owners to rights conferred by the existing legal framework (Al-Busaidi et al., 2024). With AI-generated works one of the fundamental challenges is still the difficult and relevant question of validating owners as uniquely identifiable parties (Lucchi, 2024). Given that AI systems can pursue no form of legal actions, they forfeited the right to act upon their intellectual property rights, and thus a legal lacuna. There are several copyright and patent statutes that underscore that the creator cannot be an organization (Cohen, 2017). This is problematic as no human creativity exists in a built-in capacity, for AI is autonomous; however, ownership questions remain related to ownership rights extended by copyright or patent laws.

From the point of contention that authorship of the work is a substantial facet of human creativity, the end goal of copyright laws makes ownership determinations difficult. While AI systems can independently of a provided prompt create content in some cases using automation, the notion of trying to function devoid of human inputs complicates the workings. The specificity and scope of the text prompt, or input parameters, established by the author, contribute to, of course, both the style and the quality of the creative product. That leads to the question: Is the human influence in these works of originality and distinctiveness enough merit to justify inclusion under copyright law? In terms of agency in AI-generated work, the author role has the highest impact (Lee et al., 2025); the nature of the work can be defined which provides flexibility when overseeing and can effectively track its evolution to a product that is not finalized until the feedback loop has been completed. In academic output the author's role leaves its mark of individualistic style and a perception of creative purpose.

Moreover, the range of output from AI and the distinctions between human authorship and algorithmic functions have intrinsic value (Darewych, 2023). There is no doubt in relation to the author in the transfer of final product. However, the AI algorithms for calculations in composition were not an author role, whereas of course, the unique input of human authorship as an author is a distinction of value (Craig & Kerr, 2025). The collaborative effort demonstrates the foundation of traditional notions of authorship, as well as commencing meaningful conversations about the boundaries of authorization with copyright law in our digital age.

Requiring human activity as a minimum threshold for copyrightability has practical challenges, particularly when AI is involved, challenges exist in determining how much human activity is sufficient, once again, a range here could be very wide from a human just calling upon an AI output to a human not only calling upon and AI output to curating and changing/altering significantly the AI output; but even in the most clear case, how would

a judge (in either case a judge ruling over a copyright infringement matter, or a judge ruling in an alternative dispute resolution) or a professional from law would adjudicate human threshold of activity?

When we develop approaches to inject AI copyright accountability into the potential issues with AI copyright, we maintain the notion that it is going to take some judicial and legal courage. The legal frameworks must allow rights holders and authors legal protections for their rights to their creative expression, but we also need to consider what they must innovate to deal with technological innovation. The legal systems need to supersede their existing practices, that are just at odds with the characteristics of the AI objects they protect and instead consider how they are pursuing the notions of fairness, equity and certainty (Kirakosyan, 2024). This drawing upon notions of fairness, equity (proportionality), and certainty, might either accompany or couple with actions of a principles-based, or guideline-based approach, or it prescribes a possible rationale and guidance for a person or original author attribution for AI creative acts, by leveraging ambiguities that cause some certainty for judges dealing with AI, but could also, as a consequence, start to create boundaries/formalism that creates some consistency and coherence around judging.

AI-generated works can accurately be described as an emergent novel based on transformations (creative products) made from the deployment of sophisticated algorithms and along with computational processing of data or prompts (Mohamed et al., 2024). AI-created output may rely upon existing knowledge or patterns to produce output, however, the work produced generally demonstrates an emerging novelty/originality, which is greater than the sum of its individual components (Boo et al., 2025). Just as AI can be understood as a tool or instrument within human creativity processes, individual users can also use AI to explore different means of creating art and allowing their creativity to be expressed in new modes (Ali Elfa & Dawood, 2023).

7. Impact on human creators

Creativity is often considered the distinguishing feature of being human in times of technological change, less likely to be impacted by or mitigate by disruptive technology and tagged for our future (Evans & Chen, 2023). Behavioral scientists, for example, have suggested creativity, an idea and/or product, is an artifact of humanity (Blok, 2022). Still today, generative AI applications, as in ChatGPT, will likely disrupt our uniqueness, and alter creative work of freelance or paid work (Amankwah-Amoah et al., 2024). Generative AI models leverage an immense amount of data and user inputs, which means any text, image, audio, and a combined variation can be generated (Bandi et al., 2023). This is somewhat unique in that jobs related to content delivery transpire not with human agency (writing, generating images, writing code, etc.), its workplaces propelled by jobs pertaining to delivery of information or knowledge-based content, and it is quite imaginable that generative AIs are constrained to creative work.

8. Fair Use, and Bias in AI-Generated IP

8.1. Fair use dilemmas

Copyright issues are very much at the center of the GenAI conversation (Hacohen & Elkin-Koren, 2024). More specifically, some of the more complex and ongoing issues concern the legality of using copyrighted works to train GenAI models and whether AI companies should be entitled to assert a defense of fair use (Vig, 2024). The first factor of fair use (the purpose or character of the use) evaluates two things: (i) whether the use of the original work is commercial versus non-commercial, and (ii) whether the use is transformative. To determine 'transformativeness', one must assess whether the defendant and made some new meaning, message, or purpose as to the plaintiffs (i.e. the original work).

The effects of bias and stereotypes in AI are illustrated in automated decision-making (Cossette-Lefebvre et al., 2023). Automated decision-making reflects the social thought processes that created prior practices and are therefore an accomplice to the negative stereotype and subsequent discrimination (Jan, 2023). Algorithms, for example, may be historically biased towards male candidates for a leadership role (Kyriakidou, 2025). Obviously, this is discrimination against women. Stereotyping can occur in a positive or negative context, but whichever context distortion of social reality and inequality will occur. Accordingly, bias and stereotypes are also interrelated and critical to understanding how AI can perpetuate or intensify existing social inequalities.

8.2. Bias in AI-generated creations

Bias in AI is appropriately defined as systematic and unfair preference, prejudice, preferential treatment, or bias that cause harmful, discriminatory results (Ferrara, 2023). There are three primary causes of bias in AI models: (1) data bias, when a model is trained using underrepresented data (Shahbazi et al., 2022); (2) development bias, when an AI developer's algorithms are not implemented properly in development (Xivuri & Twinomurinzi, 2023); and (3) interaction bias, when users varied their formal interactions and expectancies with the model (Grimes et al., 2021).

A major issue when justifying biases associated with AI-generated text, is that when we go back to a biased process, we are left with an invisible product often viewed as objective and neutral (e.g., the original AI is seen as having already made the choice-in that is mechanically stubborn to be scrutinized further). When readers read an AI text, comparing it to human texts, readers are expected to grant authority to authorship as the authoring of the AI text originated based on factual content-stripped of any social subjectivity, it is disillusioned at this point (with the biases re-embedded) where not only did the content originally contain the biases, but they had been confused and likely accepted as an unquestioned truth.

9. Mitigating the Risk of Generative AI IP Problem

One possibility AI developers could consider is to cover the legal ground since they are grabbing the source data, they are using to build their models (Rodríguez et al., 2023). This process should involve licensing and compensating any individuals that own the intellectual property that developers want to include in their training data through either licensing, or a portion of any revenue generated using the AI tool. Users of AI tools should inquire about the providers; if their model was trained with any protected content and consider reading the terms or use, privacy policy, and to be cautious about generative AI tools promoted by companies that cannot guarantee the training data is legally licensed to, or even open-source licenses that those companies comply with (Dwivedi et al., 2023).

9.1. Considering Potential Downstream Impacts

Artificial intelligence influences the trajectory of the broad array of cases, especially, for patent laws (Bianchini et al., 2022). Individuals using AI, either directly or through the services of a third party that includes an AI engine in their technology, is only one difficult problem for IP ownership (Picht & Thouvenin, 2023). If one person or company has asserted infringed rights, there may be thousands of others, including plaintiffs and defendants, and so forth, who might have an impact. The impact can be handled simply as ensuring you and your vendors utilize technologies that keep pace with an ever-changing environment, and even your service of process vendors can handle extreme variations in volume without impacting your delivery.

9.2. The dawn of IP Law and Artificial Intelligence

Intellectual property law and artificial intelligence together present new opportunities and issues for lawyers, businesses, and creative people (Vescovo, 2023). To be part of the future of intellectual property law and AI requires understanding and keeping up with the changing legal environment and how to face the full force of change in the new landscape called artificial intelligence, and intellectual property law. This represents a climate and environment for the law that is constantly fluid and ever-changing. Given that we are navigating a field called artificial intelligence, there is a subclass of intellectual property law that changes law and creates legal issues and questions as it changes in AI and how traditional intellectual property law is always being modified (Endeshaw, 2004).

10. Policy and Legal Recommendations

Expansion of existing regulations to require human participation in various phases of creative AI development and in the creation of works by AI. This includes defining roles

such as 'programmer, 'developer', 'operator, server', 'data author', 'data provider' and other in regulatory frameworks.

Enable contractual agreements on IP ownership pooling among parties involved. This empowers parties like programmers, developers, data authors, etc., to establish the scope of their ownership through contractual arrangements.

Need for legal entities to assume control and accountability over the works produced by AI. The goal is to prevent harm and set ethical boundaries for these systems. It is proposed to use existing studies, such as the EU study on robotics, to determine whether an author should be commissioned for works created by AI.

Treat AI-generated works as works for hire and grant rights to the person or organization commissioning the AI. However, this approach could lead to problems such as market saturation or manipulation through excessive work orders.

Current legislation recognizes the difference between human authorship and machine production and considers people who take the necessary precautions to be the creators of the works. As legal cases related to 'authorship' and 'generation' emerge, the laws governing these concepts are expected to become more refined.

Address challenges such as determining the extent of human involvement in machine-generated works and establishing the basis for human authorship of such works.

Conclusion

Copyright law offers lawyers the protection of original works of human expression. Copyright law, as it stands, does not allow for protection of AI generated works where the human contribution for originality is little or non-existent (e.g. typing a prompt). Copyright law does allow for protection of works through some use or assistance of AI depending on the overall work. It is not clear how much creativity or contribution there will need to be (or what courts require) for there to be Copyright protection of AI assisted works.

As AI technologies evolve, there will be new opportunities and challenges for protection and enforcement of intellectual property rights. The legal landscape will continue to evolve as courts and regulators deal with the challenges related to the complex and novel issues described above. The impact of AI on intellectual property has barriers and challenges but also great potential opportunities. As AI continues to evolve, it is very likely that the legal landscape will evolve as well to address the definitions and parameters of inventorship, ownership, and protection.

The field of AI and intellectual property is a fast-changing field. The legal issues surrounding AI patents, copyright issues surrounding intellectual property in AI-generated content, and trade secrets protection are just the starting point. Through advances

in AI technology, we will also witness the evolution of intellectual property laws that will need to be adaptable to provide the necessary clarity to inventors, creators, and users of AI technologies. International and other collaborative approaches, permitted by enhanced cybersecurity and ethics, will also play an important role in the future of AI and intellectual property. All stakeholders of the AI ecosystem must remain vigilant to the latest legal developments and trends, obtain professional advice from experts in this field, and take all reasonable steps to mitigate the legal risks if there are any questions.

References

Afaq, S. A., Husain, M. S., Bello, A., & Sadia, H. (2023). A critical analysis of cyber threats and their global impact. In *Computational Intelligent Security in Wireless Communications* (pp. 201–220). CRC Press. https://doi.org/10.1201/9781003323426-12

Ai, J., Gursoy, D., Liu, Y., & Lv, X. (2022). Effects of offering incentives for reviews on trust: Role of review quality and incentive source. *International Journal of Hospitality Management*, *100*, 103101. https://doi.org/10.1016/j.ijhm.2021.103101

Ajani, G. (2020). Contemporary Artificial Art and the Law: Searching for an Author. *Brill Research Perspectives in Art and Law*, *3*(4), 1–84. https://doi.org/10.1163/24519201-12340034

Al Da'jeh, A. K. M., & Alzubi, A. A. (2024). The Solutions for The Conflict of Laws Relating to Copyright and Its Exploitation «A Comparative Study». *Journal of Ecohumanism*, *3*(7), 2842–2853. https://doi.org/10.62754/joe.v3i7.4421

Al-Busaidi, A. S., Raman, R., Hughes, L., Albashrawi, M. A., Malik, T., Dwivedi, Y. K., Al- Alawi, T., AlRizeiqi, M., Davies, G., Fenwick, M., Gupta, P., Gurpur, S., Hooda, A., Jurcys, P., Lim, D., Lucchi, N., Misra, T., Raman, R., Shirish, A., & Walton, P. (2024). Redefining boundaries in innovation and knowledge domains: Investigating the impact of generative artificial intelligence on copyright and intellectual property rights. *Journal of Innovation & Knowledge*, *9*(4), 100630. https://doi.org/10.1016/j.jik.2024.100630

Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2024). AI-powered innovation in digital transformation: Key pillars and industry impact. *Sustainability*, *16*(5), 1790. https://doi.org/10.3390/su16051790

Ali Elfa, M. A., & Dawood, M. E. T. (2023). Using artificial intelligence for enhancing human creativity. *Journal of Art, Design and Music*, *2*(2), 3. https://doi.org/10.55554/2785-9649.1017

Ali, M., Khan, T. I., Khattak, M. N., & ŞENER, İ. (2024). Synergizing AI and business: Maximizing innovation, creativity, decision precision, and operational efficiency in high-tech enterprises. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(3), 100352. https://doi.org/10.1016/j.joitmc.2024.100352

Amankwah-Amoah, J., Abdalla, S., Mogaji, E., Elbanna, A., & Dwivedi, Y. K. (2024). The impending disruption of creative industries by generative AI: Opportunities, challenges, and research agenda. *International Journal of Information Management*, *79*, 102759. https://doi.org/10.1016/j.ijinfomgt.2024.102759

Arif, A., Khan, M. I., & Khan, A. R. A. (2024). An overview of cyber threats generated by AI. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 67–76. https://doi.org/10.47709/ijmdsa.v3i4.4753

Aveni, A., & Faria, L. C. (2024). Clarify Artificial Intelligence (AI) decisions models rights in Intelectual Property (IP) system. *Revista JRG de Estudos Acadêmicos*, *7*(14), e141033–e141033. https://doi.org/10.55892/jrg.v7i14.1033

Bandi, A., Adapa, P. V. S. R., & Kuchi, Y. E. V. P. K. (2023). The power of generative AI: A review of requirements, models, input–output formats, evaluation metrics, and challenges. *Future Internet*, *15*(8), 260. https://doi.org/10.3390/fi15080260

Bianchini, S., Müller, M., & Pelletier, P. (2022). Artificial intelligence in science: An emerging general method of invention. *Research Policy*, *51*(10), 104604. https://doi.org/10.1016/j.respol.2022.104604

Blok, V. (2022). The Role of Human Creativity in Human-Technology Relations. *Philosophy & Technology*, *35*, 59. https://doi.org/10.1007/s13347-022-00559-7

Boo, C., Kim, Y., & Suh, A. (2025). A Collaborative Creative Process in the Age of AI: A Comparative Analysis of Machine and Human Creativity. In *Proceedings of the 58th Hawaii International Conference on System Sciences* (pp. 212–221). https://doi.org/10.24251/hicss.2025.025

Brandenburg, J. M., Müller-Stich, B. P., Wagner, M. et al. (2025). Can surgeons trust AI? Perspectives on machine learning in surgery and the importance of eXplainable Artificial Intelligence (XAI). *Langenbeck's Archives of Surgery*, *410*, 53. https://doi.org/10.1007/s00423-025-03626-7

Castaldi, C., Giuliani, E., Kyle, M., & Nuvolari, A. (2024). Are intellectual property rights working for society? *Research Policy*, *53*(2), 104936. https://doi.org/10.1016/j.respol.2023.104936

Chaudhary, G. (2022). Artificial intelligence: copyright and authorship/ownership dilemma? *Indian Journal of Law and Justice*, *13*(2), 212.

Chen, Y., Bao, J., Weng, G., Shang, Y., Liu, C., & Jiang, B. (2024). AI-Enabled Multi-Mode Electronic Information Innovation Practice Teaching Reform Prediction and Exploration in Application-Oriented Universities. *Systems*, *12*(10), 442. https://doi.org/10.3390/systems12100442

Chesterman, S. (2025). Good models borrow, great models steal: intellectual property rights and generative AI. *Policy and Society*, *44*(1), 23–37. https://doi.org/10.1093/polsoc/puae006

Cohen, J. E. (2017). Creativity and culture in copyright theory. In *Copyright Law* (pp. 473–527). Routledge. https://doi.org/10.4324/9781315095400-17

Contreras, J. L. (2022). Ownership and Assignment of Intellectual Property. In *Intellectual Property Licensing and Transactions: Theory and Practice* (pp. 19–46). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781009049436.003

Cossette-Lefebvre, H., & Maclure, J. (2023). AI's fairness problem: understanding wrongful discrimination in the context of automated decision-making. *AI Ethics*, *3*, 1255–1269. https://doi.org/10.1007/s43681-022-00233-w

Craig, C., & Kerr, I. (2025). The death of the AI author. In *Robot Law: Volume II* (pp. 250–285). Edward Elgar Publishing. https://doi.org/10.4337/9781800887305.00014

Darewych, T. (2023). The impact of authorship on aesthetic appreciation: A study comparing human and AI-generated artworks. *Art and Society*, *2*(1), 67–73. https://doi.org/10.56397/as.2023.02.11

de la Durantaye, K. (2025). Control and Compensation. A Comparative Analysis of Copyright Exceptions for Training Generative AI. *IIC-International Review of Intellectual Property and Competition Law*, 1–34. https://doi.org/10.1007/s40319-024-01350-7

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M. K., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L. D., Buhalis, D., Carter, L. D. … et al. (2023). Opinion Paper: «So what if ChatGPT wrote it?» Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, *71*, 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642

Elkhatat, A. M., Elsaid, K., & Almeer, S. (2023). Evaluating the efficacy of AI content detection tools in differentiating between human and AI-generated text. *International Journal for Educational Integrity*, *19*(1), 17. https://doi.org/10.1007/s40979-023-00140-5

Endeshaw, A. (2004). Reconfiguring intellectual property for the information age: Towards information property. *The Journal of World Intellectual Property*, *7*, 327. https://doi.org/10.1111/j.1747-1796.2004.tb00211.x

Evans, G., & Chen, X. (2023). Creativity and Disruptive Technology. In *The Future of Responsible Management Education: University Leadership and the Digital Transformation Challenge* (pp. 19–34). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-15632-8_2

Ferrara, E. (2023). Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies. *Sci*, *6*(1), 3. https://doi.org/10.3390/sci6010003

Gaffar, H., & Albarashdi, S. (2025). Copyright protection for AI-generated works: Exploring originality and ownership in a digital landscape. *Asian Journal of International Law*, *15*(1), 23–46. https://doi.org/10.1017/s2044251323000735

Geiger, C. (2024). Elaborating a Human Rights-Friendly Copyright Framework for Generative AI. *IIC-International Review of Intellectual Property and Competition Law*, *55*(7), 1129–1165. https://doi.org/10.1007/s40319-024-01325-8

Ghiurău, D., & Popescu, D. E. (2024). Distinguishing Reality from AI: Approaches for Detecting Synthetic Content. *Computers*, *14*(1), 1. https://doi.org/10.3390/computers14010001

Giordani, J. (2024). Mitigating chatbots AI data privacy violations in the banking sector: A qualitative grounded theory study. *European Journal of Applied Science, Engineering and Technology*, *2*(4), 14–65. https://doi.org/10.59324/ejaset.2024.2(4).02

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, *7*(1), 1–15. https://doi.org/10.31235/osf.io/fj6pg

Grimes, G. M., Schuetzler, R. M., & Giboney, J. S. (2021). Mental models and expectation violations in conversational AI interactions. *Decision Support Systems*, *144*, 113515. https://doi.org/10.1016/j.dss.2021.113515

Haase, J., & Hanel, P. H. (2023). Artificial muses: Generative artificial intelligence chatbots have risen to human-level creativity. *Journal of Creativity*, *33*(3), 100066. https://doi.org/10.1016/j.yjoc.2023.100066

Hacker, P. (2023). The European AI liability directives–Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, *51*, 105871. https://doi.org/10.1016/j.clsr.2023.105871

Hacohen, U. Y., & Elkin-Koren, N. (2024). Copyright regenerated: harnessing genAI to measure originality and copyright scope. *Harvard Journal of Law & Technology*, *37*(2). https://doi.org/10.2139/ssrn.4530717

Huang, K., Wang, Y., Goertzel, B., Li, Y., Wright, S., & Ponnapalli, J. (2024). Generative AI Security. In *Future of Business and Finance*. https://doi.org/10.1007/978-3-031-54252-7

Hutson, J. (2024). The Evolving Role of Copyright Law in the Age of AI-Generated Works. *Journal of Digital Technologies and Law*, *2*(4), 886–914. https://doi.org/10.21202/jdtl.2024.43

Iguh, N. A., & Anyanor, O. E. (2023). The impact of technology and the use of the internet on copyright enforcement in Nigeria. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, *14*(2), 1–12.

Jan, A. (2023). Algorithmic Justice: Bias in Code, Bias in Society. *Journal for Social Science Studies*, *1*(2), 113–121.

Kelly, S., Kaye, S. A., White, K. M., & Oviedo-Trespalacios, O. (2023). Clearing the way for participatory data stewardship in artificial intelligence development: a mixed methods approach. *Ergonomics*, *66*(11), 1782–1799. https://doi.org/10.1080/00140139.2023.2289864

Khalaf, M. A. (2025). Does attitude towards plagiarism predict aigiarism using ChatGPT? *AI and Ethics*, *5*(1), 677–688. https://doi.org/10.1007/s43681-024-00426-5

Kim, S. (2024). Research ethics and issues regarding the use of ChatGPT-like artificial intelligence platforms by authors and reviewers: a narrative review. *Science Editing*, *11*(2), 96–106. https://doi.org/10.6087/kcse.343

Kirakosyan, A. (2024). Intellectual Property Ownership of AI-Generated Content. *Digital Law Journal*, *4*(3), 40–50. https://doi.org/10.38044/2686-9136-2023-4-3-3

Knutson, K. R. (2020). Anything you can do, AI can't do better: An analysis of conception as a requirement for patent inventorship and a rationale for excluding AI inventors. *Cybaris*, *11*(2), Article 2.

Kumar, P. (2024). Intellectual Property Rights (IPR): Nurturing Creativity, Fostering Innovation. *Idealistic Journal of Advanced Research in Progressive Spectrums (IJARPS) eISSN–2583-6986*, *3*(02), 32–38.

Kyriakidou, O. (2025). Algorithms and global diversity management. In *Research Handbook on Global Diversity Management* (pp. 148–163). Edward Elgar Publishing.

Lalanda, P., & Roig, N. A. (2025). Ethical and Legal Challenges of Artificial Intelligence with Respect to Intellectual Property. In A. Baraybar-Fernández, S. Arrufat-Martín, B. Díaz Díaz (Eds.), *The AI Revolution. Research Series on Responsible Enterprise Ecosystems* (pp. 63–80). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-80411-3_6

Lee, D. C., Jhang, J. H., & Baek, T. H. (2025). AI-Generated News Content: The Impact of AI Writer Identity and Perceived AI Human-Likeness. *International Journal of Human–Computer Interaction*, *41*(21), 13862–13874. https://doi.org/10.1080/10447318.2025.2477739

Lemley, M. A. (2024). How Generative AI Turns Copyright Upside Down. *Science and Technology Law Review*, *25*(2). https://doi.org/10.52214/stlr.v25i2.12761

Lopez, M., & Gonzalez, I. (2024). Artificial Intelligence Is Not Human: The Legal Determination of Inventorship and Co-Inventorship, the Intellectual Property of AI Inventions, and the Development of Risk Management Guidelines. *J. Pat. & Trademark Off. Soc'y*, *104*, 135.

Lovell, J. (2024). Legal Aspects of Artificial Intelligence Personhood: Exploring the Possibility of Granting Legal Personhood to Advanced Ai Systems and the Implications for Liability, Rights and Responsibilities. *International Journal of Artificial Intelligence and Machine Learning*, *4*(2), 23–40. https://doi.org/10.51483/ijaiml.4.2.2024.23-40

Lucchi, N. (2024). ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems. *European Journal of Risk Regulation*, *15*(3), 602–624. https://doi.org/10.1017/err.2023.59

Marchenko, V., Dombrovska, A., & Prodaivoda, V. (2024). Comparative Analysis of Regulatory Acts of the EU Countries on the Protection of Intellectual Property in the Conditions of the Use of Artificial Intelligence. *Public Administration and Law Review*, *3*(19), 44–66. https://doi.org/10.36690/2674-5216-2024-3-44-66

Margoni, T., & Kretschmer, M. (2022). A deeper look into the EU text and data mining exceptions: harmonisation, data ownership, and the future of technology. *GRUR international*, *71*(8), 685–701. https://doi.org/10.1093/grurint/ikac054

Marsoof, A., Luco, A. C., Tan, H. H., & Joty, S. R. (2022). Content-filtering AI systems–limitations, challenges and regulatory approaches. *Information & Communications Technology Law*, *32*, 64–101. https://doi.org/10.1080/13600834.2022.2078395

Mary, T., & Enoch, O. (2024). Legal Considerations in the Development and Commercialization of Corporate Intellectual Property. *International Journal of Rural Development, Environment and Health Research*, *8*(3), 01–20. https://doi.org/10.22161/ijreh.8.3.1

Md, S., Md Saiful, I., & Jannatul, F. (2025). Harnessing AI Adoption in the Workforce A Pathway to Sustainable Competitive Advantage through Intelligent Decision-Making and Skill Transformation. *American Journal of Economics and Business Management*, *8*(3), 954–976.

Mohamed, Y. A., Mohamed, A. H., Kannan, A., Bashir, M., Adiel, M. A., & Elsadig, M. A. (2024). Navigating the Ethical Terrain of AI-Generated Text Tools: A Review. *IEEE Access*, *12*, 197061–197120. https://doi.org/10.1109/access.2024.3521945

Obianyo, C. I. (2025). Legal challenges of artificial intelligence as a creator in patent and copyright. *Nnamdi Azikiwe University Journal of Private and Property Law*, *2*(1), 88–99.

Oda, B. (2023). No Ghost in the Machine: On Human Creativity and Why AI-Generated Images from Text Prompts Are Not Protected by Copyright. *The SciTech Lawyer*, *20*(1), 20–28.

Olaniyi, G. (2024). *Enterprise Architects Leveraging AI for Business Innovation*. https://doi.org/10.2139/ssrn.5033526

Olwan, R., & Al-Balushi, R. (2023). The Requirement of Originality in the Copyright Laws of the Arab Gulf States: Perspectives from Author's Rights Jurisdictions. *GRUR International*, *72*(11), 1030–1052. https://doi.org/10.1093/grurint/kiad065

Ooi, K. B., Tan, G. W. H., Al-Emran, M., Al-Sharafi, M. A., Capatina, A., Chakraborty, A., ... & Wong, L. W. (2025). The potential of generative artificial intelligence across disciplines: Perspectives and future directions. *Journal of Computer Information Systems*, *65*(1), 76–107. https://doi.org/10.1080/08874417.2023.2261010

Padmanabhan, A., & Wadsworth, T. J. (2024). A common law theory of ownership for AI-created properties. *Journal of the Patent and Trademark Office Society*, *104*, 155–182.

Peukert, C., & Windisch, M. (2024). The economics of copyright in the digital age. *Journal of Economic Surveys*. https://doi.org/10.1111/joes.12632

Picht, P. G., & Thouvenin, F. (2023). AI and IP: Theory to policy and back again–policy and research recommendations at the intersection of artificial intelligence and Intellectual Property. *IIC-International Review of Intellectual Property and Competition Law*, *54*(6), 916–940. https://doi.org/10.1007/s40319-023-01344-5

Pokrovskaya, A. (2025). The Legal Status of Artificial Intelligence: The Need to Form a Legal Personality and Regulate Copyright. *Artificial Intelligence and Applications*, *3*(2). https://doi.org/10.47852/bonviewaia52023901

Prakash, G., & Sabharwal, D. (2024). AI Revolution in Online Media: Transforming Content Creation, Distribution, and Consumption. *Media and AI: Navigating*, *179*.

Rodríguez, N. D., Ser, J. D., Coeckelbergh, M., Prado, M. L., Herrera-Viedma, E. E., & Herrera, F. (2023). Connecting the Dots in Trustworthy Artificial Intelligence: From AI Principles, Ethics, and Key Requirements to Responsible AI Systems and Regulation. *Information Fusion*, *99*, 101896. https://doi.org/10.1016/j.inffus.2023.101896

Rotolo, A. (2025). Human, All Too Human: A Philosophical Investigation on Intellectual Property Rights for AI-based Creativity. In *The Cyber-Creativity Process* (pp. 239–263). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-84535-2_8

Salle, S., & Rini, W. S. D. (2025). Development of artificial intelligence regulations and implications for intellectual property rights protection. *Contemporary Issues on Indonesian Social Justice and Legal Reform*, *1*(1), 58–77.

Schmit, C. D., Doerr, M. J., & Wagner, J. K. (2023). Leveraging IP for AI governance. *Science*, *379*(6633), 646–648. https://doi.org/10.1126/science.ade3743

Shahbazi, N., Lin, Y., Asudeh, A., & Jagadish, H. V. (2022). A survey on techniques for identifying and resolving representation bias in data. *CoRR, abs/2203.11852*. https://doi.org/10.48550/arXiv.2203.11852

Shalaby, A. (2024). Digital Sustainable Growth Model (DSGM): Achieving synergy between economy and technology to mitigate AGI risks and address Global debt challenges. *Journal of Economy and Technology*. https://doi.org/10.1016/j.ject.2024.08.003

Singh, S. (2024). Adapting Copyright in the Age of AI: Rethinking Authorship and Safeguarding Generative AI Work.

Srivastava, A. (2024). Asserting Ownership of Intellectual Property Rights: Protection under Intellectual Property Law. *Issue 2 Int'l JL Mgmt. & Human.*, *7*, 3593.

Tan, T. J. (2024). Artificial intelligence as inventor? *SAcLJ*, *36*, 346.

Tiwari, S. (2025). Biases and Fairness in LLMs. In *Generative AI: Techniques, Models and Applications* (pp. 229–242). Cham: Springer Nature Switzerland.

Tully, R. (2024). Who owns artificial intelligence? In *DS 131: Proceedings of the International Conference on Engineering and Product Design Education (E&PDE 2024)* (pp. 545–550). https://doi.org/10.35199/epde.2024.92

Tunç, A. (2025). Can AI determine its own future? *AI & Society*, *40*(2), 775–786. https://doi.org/10.1007/s00146-024-01939-3

Tyagi, K. (2024). Copyright, text & data mining and the innovation dimension of generative AI. *Journal of Intellectual Property Law & Practice*, *19*(7), 557–570. https://doi.org/10.1093/jiplp/jpae028

Uddagiri, C., & Isunuri, B. V. (2024). Ethical and Privacy Challenges of Generative AI. In *Generative AI: Current Trends and Applications* (pp. 219–244). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-8460-8_11

Unnikrishnan, A. (2024). Analyzing the impact of emerging technologies on intellectual property rights (IPR): a comprehensive study on the challenges and opportunities in the digital age. *Law & World*, *29*, 66. https://doi.org/10.36475/10.1.6

Varona, D., & Suárez, J. L. (2022). Discrimination, bias, fairness, and trustworthy AI. *Applied Sciences*, *12*(12), 5826. https://doi.org/10.3390/app12125826

Vărzaru, A. A., & Bocean, C. G. (2024). Digital transformation and innovation: The influence of digital technologies on turnover from innovation activities and types of innovation. *Systems*, *12*(9), 359. https://doi.org/10.3390/systems12090359

Vebritha, S. (2024). Redefining Ownership and Originality in the Age of AI: A Legal and Ethical Review. *Sinergi International Journal of Law*, *2*(4), 312–314. https://doi.org/10.61194/law.v2i4.726

Vescovo, S. (2023). Rise of the Machines: The Future of Intellectual Property Rights in the Age of Artificial Intelligence. *Brooklyn Law Review*, *89*, 221.

Vig, S. (2024). Intersection of generative artificial intelligence and copyright: an Indian perspective. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/jstpm-08-2023-0145

Walter, Y. (2024). Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences. *Discover Artificial Intelligence*, *4*, 14. https://doi.org/10.1007/s44163-024-00109-4

Wang, L., Chen, X., Deng, X., Wen, H., You, M.H., Liu, W., Li, Q., & Li, J. (2024). Prompt engineering in consistency and reliability with the evidence-based guideline for LLMs. *NPJ Digital Medicine*, *7*. https://doi.org/10.1038/s41746-024-01029-4

Werzansky-Orland, Y. (2024). AI-generated content and the question of copyright. *Market: International Journal of Business*, *5*, 2–20.

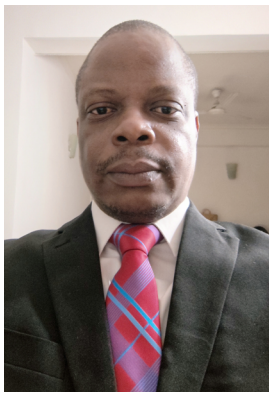
Xiao, Y. (2023). Decoding authorship: is there really no place for an algorithmic author under copyright law? *IIC-International Review of Intellectual Property and Competition Law*, *54*(1), 5–25. https://doi.org/10.1007/s40319-022-01269-5

Xiong, H. (2024). Research on confusing responses based on ChatGPT. *Applied and Computational Engineering*, *57*, 90–97. https://doi.org/10.54254/2755-2721/57/20241315

Xivuri, K., & Twinomurinzi, H. (2023). How AI developers can assure algorithmic fairness. *Discover Artificial Intelligence*, *3*(1), 27. https://doi.org/10.1007/s44163-023-00074-4

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, *55*, 1029–1053. https://doi.org/10.1007/s10462-021-09976-0

Author information



Kolawole Afuwape – LLM International Energy Law and Policy, Lecturer, Jindal Global Law School, O.P. Jindal Global University
Address: Sonipat Narela Road, Near Jagdishpur Village, Sonipat 131001, Haryana, India
E-mail: afuwapekolawole@gmail.com
ORCID ID: https://orcid.org/0009-0001-5686-230X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=59496613300
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LPP-5259-2024
Google Scholar ID: https://scholar.google.com/citations?user=2tZOhdcAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – July 25, 2025
Date of approval – August 10, 2025
Date of acceptance – December 20, 2025
Date of online placement – December 25, 2025

Научная статья
УДК 34:004:340.1:004.8:808.1:347.779
EDN: https://elibrary.ru/burdtt
DOI: https://doi.org/10.21202/jdtl.2025.27

Этические последствия применения искусственного интеллекта при создании объектов интеллектуальной собственности: проблемы авторства, владения и ответственности

Колаволе Афувапе

Глобальный университет имени О. П. Джиндала, Сонипат, Индия

Ключевые слова

авторское право,
алгоритмическая предвзятость,
генеративный искусственный интеллект,
интеллектуальная собственность,
искусственный интеллект,
патентное право,
право,
право собственности,
цифровые технологии,
этика

Аннотация

Цель: осуществить критическую оценку этических вопросов, связанных с использованием искусственного интеллекта при разработке объектов интеллектуальной собственности, с акцентом на проблемы авторства, права собственности, оригинальности и ответственности.

Методы: исследование базируется на всестороннем анализе существующей нормативной правовой базы и прецедентного права в области интеллектуальной собственности и искусственного интеллекта. Проведен систематический обзор научной литературы, включающий публикации в рецензируемых научных журналах и аналитические отчеты, посвященные этическим аспектам применения искусственного интеллекта, законодательству в сфере интеллектуальной собственности и трансформации цифрового ландшафта. Осуществлено критическое обобщение научных аргументов и теоретических дискуссий относительно этического статуса искусственного интеллекта как создателя и соавтора творческих произведений. Выполнена оценка систем искусственного интеллекта через призму концепций справедливости, подотчетности и прозрачности.

Результаты: выявлено отсутствие юридического признания искусственного интеллекта в качестве автора или изобретателя в большинстве правовых систем мира, где парадигма интеллектуальной собственности по-прежнему основана на человекоцентричных представлениях о творчестве и изобретательстве, что создает регуляторный пробел. Установлена значительная неясность в вопросах владения и подотчетности, поскольку искусственный интеллект, не обладая правосубъектностью, порождает этическое затруднение относительно того, должна ли интеллектуальная собственность, созданная автономной системой, принадлежать разработчику, пользователю, поставщику

данных или оставаться в общественном достоянии. Определены риски предвзятости и эксплуатации в креативных индустриях, где искусственный интеллект обучается с использованием материалов, защищенных авторским правом, без разрешения или компенсации их создателям. Зафиксирован переход к двойным этическим стандартам вследствие юрисдикционных и отраслевых различий в отношении произведений, созданных с помощью искусственного интеллекта, что порождает несправедливые глобальные различия в защите прав интеллектуальной собственности.

Научная новизна: представлен многогранный междисциплинарный анализ, интегрирующий правовую, этическую и технологическую сферы исследования проблематики интеллектуальной собственности, создаваемой с использованием искусственного интеллекта. Разработана концептуальная основа для комплексного решения этических и нормативных вопросов, возникающих в связи с произведениями, созданными при участии искусственного интеллекта, включая обоснование необходимости правовой реформы с учетом этических императивов современного технологического развития.

Практическая значимость: исследование содержит этически обоснованные рекомендации для законодателей, юристов-практиков и разработчиков технологий по внесению поправок в законодательство об интеллектуальной собственности, позволяющие эффективно решать вопросы авторства, права собственности и подотчетности в отношении произведений, созданных при помощи искусственного интеллекта, обеспечивая баланс между стимулированием инноваций и защитой прав человека-творца.

Для цитирования

Афувапе, К. (2025). Этические последствия применения искусственного интеллекта при создании объектов интеллектуальной собственности: проблемы авторства, владения и ответственности. *Journal of Digital Technologies and Law*, *3*(4), 677–704. https://doi.org/10.21202/jdtl.2025.27

Список литературы

Afaq, S. A., Husain, M. S., Bello, A., & Sadia, H. (2023). A critical analysis of cyber threats and their global impact. In *Computational Intelligent Security in Wireless Communications* (pp. 201–220). CRC Press. https://doi.org/10.1201/9781003323426-12

Ai, J., Gursoy, D., Liu, Y., & Lv, X. (2022). Effects of offering incentives for reviews on trust: Role of review quality and incentive source. *International Journal of Hospitality Management*, *100*, 103101. https://doi.org/10.1016/j.ijhm.2021.103101

Ajani, G. (2020). Contemporary Artificial Art and the Law: Searching for an Author. *Brill Research Perspectives in Art and Law*, *3*(4), 1–84. https://doi.org/10.1163/24519201-12340034

Al Da'jeh, A. K. M., & Alzubi, A. A. (2024). The Solutions for The Conflict of Laws Relating to Copyright and Its Exploitation «A Comparative Study». *Journal of Ecohumanism*, *3*(7), 2842–2853. https://doi.org/10.62754/joe.v3i7.4421

Al-Busaidi, A. S., Raman, R., Hughes, L., Albashrawi, M. A., Malik, T., Dwivedi, Y. K., Al- Alawi, T., AlRizeiqi, M., Davies, G., Fenwick, M., Gupta, P., Gurpur, S., Hooda, A., Jurcys, P., Lim, D., Lucchi, N., Misra, T., Raman, R., Shirish, A., & Walton, P. (2024). Redefining boundaries in innovation and knowledge domains: Investigating the impact of generative artificial intelligence on copyright and intellectual property rights. *Journal of Innovation & Knowledge*, *9*(4), 100630. https://doi.org/10.1016/j.jik.2024.100630

Aldoseri, A., Al-Khalifa, K. N., & Hamouda, A. M. (2024). AI-powered innovation in digital transformation: Key pillars and industry impact. *Sustainability*, *16*(5), 1790. https://doi.org/10.3390/su16051790

Ali Elfa, M. A., & Dawood, M. E. T. (2023). Using artificial intelligence for enhancing human creativity. *Journal of Art, Design and Music*, *2*(2), 3. https://doi.org/10.55554/2785-9649.1017

Ali, M., Khan, T. I., Khattak, M. N., & ŞENER, İ. (2024). Synergizing AI and business: Maximizing innovation, creativity, decision precision, and operational efficiency in high-tech enterprises. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(3), 100352. https://doi.org/10.1016/j.joitmc.2024.100352

Amankwah-Amoah, J., Abdalla, S., Mogaji, E., Elbanna, A., & Dwivedi, Y. K. (2024). The impending disruption of creative industries by generative AI: Opportunities, challenges, and research agenda. *International Journal of Information Management*, *79*, 102759. https://doi.org/10.1016/j.ijinfomgt.2024.102759

Arif, A., Khan, M. I., & Khan, A. R. A. (2024). An overview of cyber threats generated by AI. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 67–76. https://doi.org/10.47709/ijmdsa.v3i4.4753

Aveni, A., & Faria, L. C. (2024). Clarify Artificial Intelligence (AI) decisions models rights in Intelectual Property (IP) system. *Revista JRG de Estudos Acadêmicos*, *7*(14), e141033–e141033. https://doi.org/10.55892/jrg.v7i14.1033

Bandi, A., Adapa, P. V. S. R., & Kuchi, Y. E. V. P. K. (2023). The power of generative AI: A review of requirements, models, input–output formats, evaluation metrics, and challenges. *Future Internet*, *15*(8), 260. https://doi.org/10.3390/fi15080260

Bianchini, S., Müller, M., & Pelletier, P. (2022). Artificial intelligence in science: An emerging general method of invention. *Research Policy*, *51*(10), 104604. https://doi.org/10.1016/j.respol.2022.104604

Blok, V. (2022). The Role of Human Creativity in Human-Technology Relations. *Philosophy & Technology*, *35*, 59. https://doi.org/10.1007/s13347-022-00559-7

Boo, C., Kim, Y., & Suh, A. (2025). A Collaborative Creative Process in the Age of AI: A Comparative Analysis of Machine and Human Creativity. In *Proceedings of the 58th Hawaii International Conference on System Sciences* (pp. 212–221). https://doi.org/10.24251/hicss.2025.025

Brandenburg, J. M., Müller-Stich, B. P., Wagner, M. et al. (2025). Can surgeons trust AI? Perspectives on machine learning in surgery and the importance of eXplainable Artificial Intelligence (XAI). *Langenbeck's Archives of Surgery*, *410*, 53. https://doi.org/10.1007/s00423-025-03626-7

Castaldi, C., Giuliani, E., Kyle, M., & Nuvolari, A. (2024). Are intellectual property rights working for society? *Research Policy*, *53*(2), 104936. https://doi.org/10.1016/j.respol.2023.104936

Chaudhary, G. (2022). Artificial intelligence: copyright and authorship/ownership dilemma? *Indian Journal of Law and Justice*, *13*(2), 212.

Chen, Y., Bao, J., Weng, G., Shang, Y., Liu, C., & Jiang, B. (2024). AI-Enabled Multi-Mode Electronic Information Innovation Practice Teaching Reform Prediction and Exploration in Application-Oriented Universities. *Systems*, *12*(10), 442. https://doi.org/10.3390/systems12100442

Chesterman, S. (2025). Good models borrow, great models steal: intellectual property rights and generative AI. *Policy and Society*, *44*(1), 23–37. https://doi.org/10.1093/polsoc/puae006

Cohen, J. E. (2017). Creativity and culture in copyright theory. In *Copyright Law* (pp. 473–527). Routledge. https://doi.org/10.4324/9781315095400-17

Contreras, J. L. (2022). Ownership and Assignment of Intellectual Property. In *Intellectual Property Licensing and Transactions: Theory and Practice* (pp. 19–46). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781009049436.003

Cossette-Lefebvre, H., & Maclure, J. (2023). AI's fairness problem: understanding wrongful discrimination in the context of automated decision-making. *AI Ethics*, *3*, 1255–1269. https://doi.org/10.1007/s43681-022-00233-w

Craig, C., & Kerr, I. (2025). The death of the AI author. In *Robot Law: Volume II* (pp. 250–285). Edward Elgar Publishing. https://doi.org/10.4337/9781800887305.00014

Darewych, T. (2023). The impact of authorship on aesthetic appreciation: A study comparing human and AI-generated artworks. *Art and Society*, *2*(1), 67–73. https://doi.org/10.56397/as.2023.02.11

de la Durantaye, K. (2025). Control and Compensation. A Comparative Analysis of Copyright Exceptions for Training Generative AI. *IIC-International Review of Intellectual Property and Competition Law*, 1–34. https://doi.org/10.1007/s40319-024-01350-7

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M. K., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L. D., Buhalis, D., Carter, L. D. … et al. (2023). Opinion Paper: «So what if ChatGPT wrote it?» Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, *71*, 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642

Elkhatat, A. M., Elsaid, K., & Almeer, S. (2023). Evaluating the efficacy of AI content detection tools in differentiating between human and AI-generated text. *International Journal for Educational Integrity*, *19*(1), 17. https://doi.org/10.1007/s40979-023-00140-5

Endeshaw, A. (2004). Reconfiguring intellectual property for the information age: Towards information property. *The Journal of World Intellectual Property*, *7*, 327. https://doi.org/10.1111/j.1747-1796.2004.tb00211.x

Evans, G., & Chen, X. (2023). Creativity and Disruptive Technology. In *The Future of Responsible Management Education: University Leadership and the Digital Transformation Challenge* (pp. 19–34). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-15632-8_2

Ferrara, E. (2023). Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies. *Sci*, *6*(1), 3. https://doi.org/10.3390/sci6010003

Gaffar, H., & Albarashdi, S. (2025). Copyright protection for AI-generated works: Exploring originality and ownership in a digital landscape. *Asian Journal of International Law*, *15*(1), 23–46. https://doi.org/10.1017/s2044251323000735

Geiger, C. (2024). Elaborating a Human Rights-Friendly Copyright Framework for Generative AI. *IIC-International Review of Intellectual Property and Competition Law*, *55*(7), 1129–1165. https://doi.org/10.1007/s40319-024-01325-8

Ghiurău, D., & Popescu, D. E. (2024). Distinguishing Reality from AI: Approaches for Detecting Synthetic Content. *Computers*, *14*(1), 1. https://doi.org/10.3390/computers14010001

Giordani, J. (2024). Mitigating chatbots AI data privacy violations in the banking sector: A qualitative grounded theory study. *European Journal of Applied Science, Engineering and Technology*, *2*(4), 14–65. https://doi.org/10.59324/ejaset.2024.2(4).02

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, *7*(1), 1–15. https://doi.org/10.31235/osf.io/fj6pg

Grimes, G. M., Schuetzler, R. M., & Giboney, J. S. (2021). Mental models and expectation violations in conversational AI interactions. *Decision Support Systems*, *144*, 113515. https://doi.org/10.1016/j.dss.2021.113515

Haase, J., & Hanel, P. H. (2023). Artificial muses: Generative artificial intelligence chatbots have risen to human-level creativity. *Journal of Creativity*, *33*(3), 100066. https://doi.org/10.1016/j.yjoc.2023.100066

Hacker, P. (2023). The European AI liability directives–Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, *51*, 105871. https://doi.org/10.1016/j.clsr.2023.105871

Hacohen, U. Y., & Elkin-Koren, N. (2024). Copyright regenerated: harnessing genAI to measure originality and copyright scope. *Harvard Journal of Law & Technology*, *37*(2). https://doi.org/10.2139/ssrn.4530717

Huang, K., Wang, Y., Goertzel, B., Li, Y., Wright, S., & Ponnapalli, J. (2024). Generative AI Security. In *Future of Business and Finance*. https://doi.org/10.1007/978-3-031-54252-7

Hutson, J. (2024). The Evolving Role of Copyright Law in the Age of AI-Generated Works. *Journal of Digital Technologies and Law*, *2*(4), 886–914. https://doi.org/10.21202/jdtl.2024.43

Iguh, N. A., & Anyanor, O. E. (2023). The impact of technology and the use of the internet on copyright enforcement in Nigeria. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, *14*(2), 1–12.

Jan, A. (2023). Algorithmic Justice: Bias in Code, Bias in Society. *Journal for Social Science Studies*, *1*(2), 113–121.

Kelly, S., Kaye, S. A., White, K. M., & Oviedo-Trespalacios, O. (2023). Clearing the way for participatory data stewardship in artificial intelligence development: a mixed methods approach. *Ergonomics*, *66*(11), 1782–1799. https://doi.org/10.1080/00140139.2023.2289864

Khalaf, M. A. (2025). Does attitude towards plagiarism predict aigiarism using ChatGPT? *AI and Ethics*, *5*(1), 677–688. https://doi.org/10.1007/s43681-024-00426-5

Kim, S. (2024). Research ethics and issues regarding the use of ChatGPT-like artificial intelligence platforms by authors and reviewers: a narrative review. *Science Editing*, *11*(2), 96–106. https://doi.org/10.6087/kcse.343

Kirakosyan, A. (2024). Intellectual Property Ownership of AI-Generated Content. *Digital Law Journal*, *4*(3), 40–50. https://doi.org/10.38044/2686-9136-2023-4-3-3

Knutson, K. R. (2020). Anything you can do, AI can't do better: An analysis of conception as a requirement for patent inventorship and a rationale for excluding AI inventors. *Cybaris*, *11*(2), Article 2.

Kumar, P. (2024). Intellectual Property Rights (IPR): Nurturing Creativity, Fostering Innovation. *Idealistic Journal of Advanced Research in Progressive Spectrums (IJARPS) eISSN–2583-6986*, *3*(02), 32–38.

Kyriakidou, O. (2025). Algorithms and global diversity management. In *Research Handbook on Global Diversity Management* (pp. 148–163). Edward Elgar Publishing.

Lalanda, P., & Roig, N. A. (2025). Ethical and Legal Challenges of Artificial Intelligence with Respect to Intellectual Property. In A. Baraybar-Fernández, S. Arrufat-Martín, B. Díaz Díaz (Eds.), *The AI Revolution. Research Series on Responsible Enterprise Ecosystems* (pp. 63–80). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-80411-3_6

Lee, D. C., Jhang, J. H., & Baek, T. H. (2025). AI-Generated News Content: The Impact of AI Writer Identity and Perceived AI Human-Likeness. *International Journal of Human–Computer Interaction*, *41*(21), 13862–13874. https://doi.org/10.1080/10447318.2025.2477739

Lemley, M. A. (2024). How Generative AI Turns Copyright Upside Down. *Science and Technology Law Review*, *25*(2). https://doi.org/10.52214/stlr.v25i2.12761

Lopez, M., & Gonzalez, I. (2024). Artificial Intelligence Is Not Human: The Legal Determination of Inventorship and Co-Inventorship, the Intellectual Property of AI Inventions, and the Development of Risk Management Guidelines. *J. Pat. & Trademark Off. Soc'y*, *104*, 135.

Lovell, J. (2024). Legal Aspects of Artificial Intelligence Personhood: Exploring the Possibility of Granting Legal Personhood to Advanced Ai Systems and the Implications for Liability, Rights and Responsibilities. *International Journal of Artificial Intelligence and Machine Learning*, *4*(2), 23–40. https://doi.org/10.51483/ijaiml.4.2.2024.23-40

Lucchi, N. (2024). ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems. *European Journal of Risk Regulation*, *15*(3), 602–624. https://doi.org/10.1017/err.2023.59

Marchenko, V., Dombrovska, A., & Prodaivoda, V. (2024). Comparative Analysis of Regulatory Acts of the EU Countries on the Protection of Intellectual Property in the Conditions of the Use of Artificial Intelligence. *Public Administration and Law Review*, *3*(19), 44–66. https://doi.org/10.36690/2674-5216-2024-3-44-66

Margoni, T., & Kretschmer, M. (2022). A deeper look into the EU text and data mining exceptions: harmonisation, data ownership, and the future of technology. *GRUR international*, *71*(8), 685–701. https://doi.org/10.1093/grurint/ikac054

Marsoof, A., Luco, A. C., Tan, H. H., & Joty, S. R. (2022). Content-filtering AI systems–limitations, challenges and regulatory approaches. *Information & Communications Technology Law*, *32*, 64–101. https://doi.org/10.1080/13600834.2022.2078395

Mary, T., & Enoch, O. (2024). Legal Considerations in the Development and Commercialization of Corporate Intellectual Property. *International Journal of Rural Development, Environment and Health Research*, *8*(3), 01–20. https://doi.org/10.22161/ijreh.8.3.1

Md, S., Md Saiful, I., & Jannatul, F. (2025). Harnessing AI Adoption in the Workforce A Pathway to Sustainable Competitive Advantage through Intelligent Decision-Making and Skill Transformation. *American Journal of Economics and Business Management*, *8*(3), 954–976.

Mohamed, Y. A., Mohamed, A. H., Kannan, A., Bashir, M., Adiel, M. A., & Elsadig, M. A. (2024). Navigating the Ethical Terrain of AI-Generated Text Tools: A Review. *IEEE Access*, *12*, 197061–197120. https://doi.org/10.1109/access.2024.3521945

Obianyo, C. I. (2025). Legal challenges of artificial intelligence as a creator in patent and copyright. *Nnamdi Azikiwe University Journal of Private and Property Law*, *2*(1), 88–99.

Oda, B. (2023). No Ghost in the Machine: On Human Creativity and Why AI-Generated Images from Text Prompts Are Not Protected by Copyright. *The SciTech Lawyer*, *20*(1), 20–28.

Olaniyi, G. (2024). *Enterprise Architects Leveraging AI for Business Innovation*. https://doi.org/10.2139/ssrn.5033526

Olwan, R., & Al-Balushi, R. (2023). The Requirement of Originality in the Copyright Laws of the Arab Gulf States: Perspectives from Author's Rights Jurisdictions. *GRUR International*, *72*(11), 1030–1052. https://doi.org/10.1093/grurint/kiad065

Ooi, K. B., Tan, G. W. H., Al-Emran, M., Al-Sharafi, M. A., Capatina, A., Chakraborty, A., ... & Wong, L. W. (2025). The potential of generative artificial intelligence across disciplines: Perspectives and future directions. *Journal of Computer Information Systems*, *65*(1), 76–107. https://doi.org/10.1080/08874417.2023.2261010

Padmanabhan, A., & Wadsworth, T. J. (2024). A common law theory of ownership for AI-created properties. *Journal of the Patent and Trademark Office Society*, *104*, 155–182.

Peukert, C., & Windisch, M. (2024). The economics of copyright in the digital age. *Journal of Economic Surveys*. https://doi.org/10.1111/joes.12632

Picht, P. G., & Thouvenin, F. (2023). AI and IP: Theory to policy and back again–policy and research recommendations at the intersection of artificial intelligence and Intellectual Property. *IIC-International Review of Intellectual Property and Competition Law*, *54*(6), 916–940. https://doi.org/10.1007/s40319-023-01344-5

Pokrovskaya, A. (2025). The Legal Status of Artificial Intelligence: The Need to Form a Legal Personality and Regulate Copyright. *Artificial Intelligence and Applications*, *3*(2). https://doi.org/10.47852/bonviewaia52023901

Prakash, G., & Sabharwal, D. (2024). AI Revolution in Online Media: Transforming Content Creation, Distribution, and Consumption. *Media and AI: Navigating*, *179*.

Rodríguez, N. D., Ser, J. D., Coeckelbergh, M., Prado, M. L., Herrera-Viedma, E. E., & Herrera, F. (2023). Connecting the Dots in Trustworthy Artificial Intelligence: From AI Principles, Ethics, and Key Requirements to Responsible AI Systems and Regulation. *Information Fusion*, *99*, 101896. https://doi.org/10.1016/j.inffus.2023.101896

Rotolo, A. (2025). Human, All Too Human: A Philosophical Investigation on Intellectual Property Rights for AI-based Creativity. In *The Cyber-Creativity Process* (pp. 239–263). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-84535-2_8

Salle, S., & Rini, W. S. D. (2025). Development of artificial intelligence regulations and implications for intellectual property rights protection. *Contemporary Issues on Indonesian Social Justice and Legal Reform*, *1*(1), 58–77.

Schmit, C. D., Doerr, M. J., & Wagner, J. K. (2023). Leveraging IP for AI governance. *Science*, *379*(6633), 646–648. https://doi.org/10.1126/science.ade3743

Shahbazi, N., Lin, Y., Asudeh, A., & Jagadish, H. V. (2022). A survey on techniques for identifying and resolving representation bias in data. *CoRR, abs/2203.11852*. https://doi.org/10.48550/arXiv.2203.11852

Shalaby, A. (2024). Digital Sustainable Growth Model (DSGM): Achieving synergy between economy and technology to mitigate AGI risks and address Global debt challenges. *Journal of Economy and Technology*. https://doi.org/10.1016/j.ject.2024.08.003

Singh, S. (2024). Adapting Copyright in the Age of AI: Rethinking Authorship and Safeguarding Generative AI Work.

Srivastava, A. (2024). Asserting Ownership of Intellectual Property Rights: Protection under Intellectual Property Law. *Issue 2 Int'l JL Mgmt. & Human.*, *7*, 3593.

Tan, T. J. (2024). Artificial intelligence as inventor? *SAcLJ*, *36*, 346.

Tiwari, S. (2025). Biases and Fairness in LLMs. In *Generative AI: Techniques, Models and Applications* (pp. 229–242). Cham: Springer Nature Switzerland.

Tully, R. (2024). Who owns artificial intelligence? In *DS 131: Proceedings of the International Conference on Engineering and Product Design Education (E&PDE 2024)* (pp. 545–550). https://doi.org/10.35199/epde.2024.92

Tunç, A. (2025). Can AI determine its own future? *AI & Society*, *40*(2), 775–786. https://doi.org/10.1007/s00146-024-01939-3

Tyagi, K. (2024). Copyright, text & data mining and the innovation dimension of generative AI. *Journal of Intellectual Property Law & Practice*, *19*(7), 557–570. https://doi.org/10.1093/jiplp/jpae028

Uddagiri, C., & Isunuri, B. V. (2024). Ethical and Privacy Challenges of Generative AI. In *Generative AI: Current Trends and Applications* (pp. 219–244). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-8460-8_11

Unnikrishnan, A. (2024). Analyzing the impact of emerging technologies on intellectual property rights (IPR): a comprehensive study on the challenges and opportunities in the digital age. *Law & World*, *29*, 66. https://doi.org/10.36475/10.1.6

Varona, D., & Suárez, J. L. (2022). Discrimination, bias, fairness, and trustworthy AI. *Applied Sciences*, *12*(12), 5826. https://doi.org/10.3390/app12125826

Vărzaru, A. A., & Bocean, C. G. (2024). Digital transformation and innovation: The influence of digital technologies on turnover from innovation activities and types of innovation. *Systems*, *12*(9), 359. https://doi.org/10.3390/systems12090359

Vebritha, S. (2024). Redefining Ownership and Originality in the Age of AI: A Legal and Ethical Review. *Sinergi International Journal of Law*, *2*(4), 312–314. https://doi.org/10.61194/law.v2i4.726

Vescovo, S. (2023). Rise of the Machines: The Future of Intellectual Property Rights in the Age of Artificial Intelligence. *Brooklyn Law Review*, *89*, 221.

Vig, S. (2024). Intersection of generative artificial intelligence and copyright: an Indian perspective. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/jstpm-08-2023-0145

Walter, Y. (2024). Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences. *Discover Artificial Intelligence*, *4*, 14. https://doi.org/10.1007/s44163-024-00109-4

Wang, L., Chen, X., Deng, X., Wen, H., You, M.H., Liu, W., Li, Q., & Li, J. (2024). Prompt engineering in consistency and reliability with the evidence-based guideline for LLMs. *NPJ Digital Medicine*, *7*. https://doi.org/10.1038/s41746-024-01029-4

Werzansky-Orland, Y. (2024). AI-generated content and the question of copyright. *Market: International Journal of Business*, *5*, 2–20.

Xiao, Y. (2023). Decoding authorship: is there really no place for an algorithmic author under copyright law? *IIC-International Review of Intellectual Property and Competition Law*, *54*(1), 5–25. https://doi.org/10.1007/s40319-022-01269-5

Xiong, H. (2024). Research on confusing responses based on ChatGPT. *Applied and Computational Engineering*, *57*, 90–97. https://doi.org/10.54254/2755-2721/57/20241315

Xivuri, K., & Twinomurinzi, H. (2023). How AI developers can assure algorithmic fairness. *Discover Artificial Intelligence*, *3*(1), 27. https://doi.org/10.1007/s44163-023-00074-4

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, *55*, 1029–1053. https://doi.org/10.1007/s10462-021-09976-0

Сведения об авторе

Афувапе Колаволе – магистр права в области международного энергетического права, преподаватель, Школа права, Глобальный университет им. О. П. Джиндала
Адрес: 131001, Индия, Харьяна, г. Сонипат, район Джагдишпур, ул. Сонипат Нарел
E-mail: afuwapekolawole@gmail.com
ORCID ID: https://orcid.org/0009-0001-5686-230X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=59496613300
WoS Researcher ID: https://www.webofscience.com/wos/author/record/LPP-5259-2024
Google Scholar ID: https://scholar.google.com/citations?user=2tZOhdcAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 25 июля 2025 г.
Дата одобрения после рецензирования – 10 августа 2025 г.
Дата принятия к опубликованию – 20 декабря 2025 г.
Дата онлайн-размещения – 25 декабря 2025 г.

Research article
UDC 34:004:346.6:004.8:004.896:349.2
EDN: https://elibrary.ru/vluyug
DOI: https://doi.org/10.21202/jdtl.2025.28

Robot Taxation as a Tool for Labor Market Protection: Legal Analysis of the Prospects for Developing Economies by the Example of Nigeria

Deborah Elohozino Otighi
Redeemer's University, Ede, Nigeria

Keywords

artificial intelligence,
digital technologies,
employment,
labor market,
labor relations,
law,
robotics,
tax,
tax law,
taxation

Abstract

Objective: to provide a comprehensive legal and economic analysis of the validity of robot taxation as a measure to protect the labor market under the increasing automation, taking into account the socio-economic realities of Nigeria's developing economy.

Methods: the research is based on doctrinal and comparative legal methodology. The author systematically analyzed scientific publications, legislative acts, statistical data and empirical materials related to the impact of robotics and artificial intelligence on global labor markets. Special attention was paid to studying tax policy in the field of automation in South Korea and the European Union, in order to identify universal patterns and specific features of automation regulation in various jurisdictions. Methodological tools include content analysis of regulatory documents, economic and statistical analysis of data from international organizations, and a critical analysis of doctrinal provisions regarding the prospects for robot taxation.

Results: the research demonstrates the ambiguity of the robot taxation institute in the modern legal and economic system. It was found that the robot taxation may slow down the pace of automation, provide workers with time to adapt and retrain, compensate for the reduction in income tax revenues and ensure economic equity by redistributing corporate income from automation. At the same time, significant limitations of this concept were identified: the risk of inhibiting innovation, the lack of a unified

legal definition of the "robot", the threat of capital outflow and the shift of production to jurisdictions with a more favorable tax environment. In relation to Nigeria, the conclusion is that a robot tax is premature due to low automation, high structural unemployment, the dominance of the informal employment sector, and poor digital infrastructure.

Scientific novelty: the work is a systematic study of the legal and economic aspects of robot taxation in the Nigerian legal system. The study is novel as it substantiates a contextual approach to determining the feasibility of a robot tax, taking into account the stage of economic development, the structure of the labor market and the degree of penetration of automation technologies. For the first time, the author formulates the concept of responsible automation for developing economies, which implies not punitive taxation, but a system of incentives combining moderate fees with investments in human capital and digital infrastructure.

Practical significance: the research results are valuable for forming state policy in the field of labor automation regulation. The proposed recommendations include the reform of corporate tax codes taking into account responsible automation, the introduction of mandatory assessment of the impact of automation on employment, the creation of a system of tax incentives for companies retraining workers displaced by technology, and the formation of a multilateral platform for ethical automation management. They can be used by the legislative and executive authorities of Nigeria and other developing countries to create legal mechanisms for regulating the digital economy and protecting workers' rights under the technological transformation

For citation

Otighi, D. El. (2025). Safeguarding the future of work in Nigeria: robot taxation in the age of automation. *Journal of Digital Technologies and Law, 3*(4), 705–721. https://doi.org/10.21202/jdtl.2025.28

Contents

Introduction

In the rapidly evolving world of labour, automation and robotics are reshaping the very foundation of the labour markets globally. Technology continually transforms the global workforce, replacing traditional jobs with automated systems (Rayhan, 2023). Over the past decade, the global stock of industrial robots has risen dramatically and is projected to grow even faster in the next 10 years[1]. By 2030, robots and artificial intelligence are projected to displace over 20 million manufacturing jobs globally – a seismic shift that threatens to exacerbate inequalities, leaving workers stranded without viable means of livelihood[2]. While these technologies in some ways offer significant gains, such as increased efficiency and reduction of business costs, to others, they pose a critical socio-economic dilemma, ethical issues, and legal concerns for governments, threatening human workers. Hence, Bill Gates, co-founder of Microsoft, in 2017, re-echoed the proposal of a robot tax to slow automation and fund workers' retraining programmes.

Currently, no country has fully implemented a robot tax in its pure form; however, policy experiments have often taken the shape of incentive reductions or broader tax reforms rather than direct levies on automation. For a developing country such as Nigeria, where the unemployment rate has consistently exceeded 30%[3], automation and the implementation of robot tax present both an opportunity and a challenge. Industries such as banking, manufacturing, and legal services are integrating technology. However, it still raises concerns about job security – should the government implement robot taxes to protect human workers? Within this discussion, the term robot will be categorised as industrial robots and actual AI-driven automation systems in labour practices (Gaus & Hoxtell, 2019; Graetz & Michaels, 2018; Guerreiro et al, 2023).

1. Understanding Robot Tax: Definition and Rationale

The concept of robot tax stems from taxing companies that heavily rely on automation, robots and AI for their operational activities. As of the 2023 reports by the International Federation of Robotics, there had been 553,052 industrial robot installations in factories

1 In developed nations, self-checkout kiosks have replaced cashiers, AI-powered chatbots handle customer service inquiries, and industrial robots now perform complex manufacturing tasks.

2 Lambart, J., & Cones, E. (2019, June 26). How Robots Change the World: What Automation Really Means for Jobs and Productivity. Oxford Economics. https://clck.ru/3QmTfr

3 Mbachu, D. (2025, February 13). Nigeria's revamp of economic indicators sparks debate' African Business. https://clck.ru/3QmTis

around the world – a growth rate of 5% from the previous year, with China being the world's largest market[4]. Hence, as taxation is imposed on workers based on income earned, companies that deploy robots capable of autonomous decision-making are taxed to the degree to which they are deployed. The term can refer to a proposed fiscal policy where companies that replace human workers with robots or automation systems are taxed either directly on using those systems or indirectly through adjustments to corporate tax rates.

The central aim of levying this tax is to serve as a legislative strategy to disincentivise the replacement of workers by machines, bolster the social safety net for those who are displaced, redistribute the economic gains from technological progress by supporting workers displaced by automation, and enhance societal equity[5]. Broadly, robot tax proposals have classified these taxes into three categories, which are;

A. The direct taxation of firms that benefit from taxes levied on a robot's hypothetical 'salary' based on calculations of the robot's productivity, or the AI automation tools, and the wages that would be paid to a human worker doing the same job (Prettner & Strulik, 2020).

B. Tax is levied on the use of robots rather than the robots[6]. This category connotes the usage-based levy, which depends primarily on how extensively firms deploy automation in their operations.

C. The 'markup' corporate tax will be levied on excess profits generated when robots and AI are used to enhance market power[7]. This adjusted corporate model increases tax rates on profits derived from high-level automation, especially where such automation contributes to job displacement.

2. Exploring the Case for Robot Taxation

With a clearer understanding of what robot taxation entails and the objectives it seeks to achieve, it is now important to assess the main arguments made in support. Thus, this section explores these propositions and their broader policy implication.

---

4 Heer, C., & Bieller, S. (2023, September 26). World Robotics 2023 Report: Asia ahead of Europe and the Americas. IFR Press Room. https://clck.ru/3QmTko. This number would have grown by now in 2025 when this paper was written.

5 Ahn, M. (2024, May 13). Navigating the Future of Work: A case of a Robot Tax in the age of AI. Brookings Institution. https://clck.ru/3QmTnc

6 In this case, firms would pay for the negative externalities of using robots instead of humans, and the value of robots is assessed according to the income they generate and taxed accordingly. Essentially, this proposal is akin to a property tax, which is based on evaluating depreciable assets and avoids the potential stagnation of innovation.

7 Morinobu, Sh. (2022, June 28). Can a Robot Tax Help Narrow the Social Divide? The Tokyo Foundation. https://clck.ru/3QmTtQ

2.1. Slowing Job Displacement to Protect Labour Markets

One of the strongest propositions for robot tax is its potential to mitigate mass unemployment in the workforce, ensure job protection and maintain economic stability[8]. The International Labour Law standard defines a worker in the workforce as someone who performs work for remuneration or profit for a minimum period, often at least one hour, within a specific reference period (Creighton & McCrystal, 2016). The central issue here is that as technology advances, more jobs are becoming obsolete, displacing human workers who are not in tandem with the multifaceted capabilities of robotics, leading to retrenchments and job losses. Recent data from the Organisation for Economic Co-operation and Development (OECD) in 2024 shows that employment and labour force participation across member countries reached historic highs with 70.3% and 74% respectively, and the unemployment rate fell to just 4.9%. Nevertheless, amid this market performance, concerns persist about automation's long-term effects, particularly its silent displacement of workers in routine and low-skilled roles[9]. Machines are increasingly capable of performing the mundane and even highly specialised tasks once reserved for humans. So, corporations would safely pick an investment in robots over human workers, leaving millions of jobs at risk[10].

Thus, a government robot tax could help slow down the automation rate, giving workers sufficient time to adapt and upskill and for the government to develop support systems for human labour (Carbonara et al, 2024; Costinot & Werning, 2022). Undoubtedly, it would serve as a cushioning policy and regulatory pause button in the face of technological advancement[11], while economic and welfare plans for displaced workers are made. For countries with limited social security systems and high youth employment rates, such as Nigeria, this will be critical because, without deliberate intervention, automation may worsen social instability, drive unemployment and intensify migration pressures. A robot tax allows policymakers to create transformative and comprehensive labour market policies, including upskilling strategies and inclusive digital education reforms. It could also open doors for laws requiring companies to conduct automation impact assessments before laying off workers.

---

8 Korner, K., Schattenberg, M., & Heymann, E. (2018, May). Digital Economics. How AI and Robotics are Changing our Work and our Lives. EU Monitor. https://clck.ru/3QnAgv

9 OECD. (2025, January 16). OECD employment and labour force participation rates stable at record highs in the third quarter of 2024. https://clck.ru/3QmU2q

10 Mitha, S. (2017, September 14). Robots, Technological Change and Taxation. (1368) Tax Journal. https://clck.ru/3QmU9h

11 Damijan, J., Damijan, S., & Vrh, N. (2021, March 9). Tax on robots: Whether and How much. Growinpro. Working Paper. 5/2021. https://clck.ru/3QmUBZ

2.2. Compensation for Declining Income Tax Revenues

As fewer people work due to automation, income tax collection by the government will naturally shrink. Hence, this argument is centred on the premise that a robot tax could aid the government in funding social programs that better equip displaced workers with new skills. It is well known that taxation is one of the most excellent means of revenue generation among world nations (Adekanmbi et al., 2024). As robots become more prevalent in the workforce, income tax may significantly decline, which would be detrimental to this germane source of governmental revenue (Mazur, 2019).

However, the robot tax offers a novel and interesting stream for the government, which must ensure its citizens' welfare and security on retained fiscal capacity (Abbott & Bogenschneider, 2018). A robot tax helps plug this gap by shifting the tax burden partly onto firms that automate. Consequently, the revenue generated from robot taxes could be reinvested in digital education, core vocational training and employment transition initiatives (Thuemmel, 2023; Zhang, 2019; Zhang, 2021). The implication is that robot taxation offers a long-term fiscal sustainability strategy, especially for tax systems overly reliant on payroll contributions as part of a broader tax reform and revenue diversification for future-proof governance.

2.3. Ensuring Equity in Corporate Gains from Automation

Another justification for the robot tax is ensuring corporate ethical accountability and fairness anchored on economic justice (Dimitropoulou, 2024). Economic justice is a component of social and welfare economics that seeks to provide avenues for financial prosperity and equality to individuals who have been marginalised in an economy[12]. For instance, if a multinational company replaces 100 workers with robots, it has saved significantly on salaries, health benefits and even pensions. By general principles of law and equity, these robot replacements do not pay tax as the law does not recognise them as taxable persons, creating imbalances as companies are not taxed on the basis of the profits accrued. More so, results from the 2022 McKinsey Global Industrial Robotics Survey reveal that industrial companies are set to spend heavily on robotics and automation[13].

Thus, on the precepts of economic justice, a robot tax would act as a redistributive mechanism in correcting these systemic imbalances by ensuring that companies that

[12] Hayes, A. (2023, September 13). Economic Justice: Meaning, Examples of How to Achieve It. Investopedia. https://clck.ru/3QmUMv

[13] Ajewole, F., Kelkar, A., Moore, D., Shao, E., & Thirtha, M. (2023, January 6). Unlocking the Industrial Potential of Robotics and Automation. McKinsey & Company. https://clck.ru/3QmUQr

benefit from automation contribute to the social and economic systems that keep society alive and functioning[14]. A study by economists at the Massachusetts Institute of Technology suggests a robot levy, but only a modest one, could help combat the effects of automation on income inequality in the U.S. if it ranges from 1 per cent to 3.7 per cent of the robot's value[15]. Hence, implementing such a tax could form part of corporate responsibility legislation, encouraging fairer profits investment into human capital development.

3. Challenges and Critiques of Robot Taxation

While the case for robot taxation continues to gain traction in public discourse, it is not without significant criticism. There are concerns about the practical, economic, and ethical ramifications of such a tax, particularly in developing countries with fragile economies and low automation levels. Hence, this section evaluates these counterarguments and potential drawbacks of implementing robot taxes.

3.1. Risk of Stifling Innovation and Technological Adoption

One of the most vigorous counterarguments is that robot taxes may stifle innovation, productivity, and technological advancement, especially in developing economies trying to match the global pace, by penalising productivity against the economic growth it brings[16]. In this context, for these economies, the robot tax is viewed as a punishment by the government instead of a blessing for attaining technological prowess, even benefiting the nation. In developing countries where blooming industries like agriculture, transport, tourism, and fintech are only beginning to adopt automation, the government implementing robot taxes on intelligent systems may prove overly premature and counterproductive, creating additional financial barriers (Mazur, 2024).

The economic implication of this thought is that robot taxation may signal a policy hostility to innovation, which could deter foreign jurisdictional investment in AI and robotics, and slow down much-needed industrial modernisation (Kovacev, 2020) which already positively impact core sectors like healthcare, where AI Robotics diagnostics save lives and detect cancers earlier than human practitioners. Also, robot taxes limit and remove the potential to develop and create new jobs. In the words of Joseph Schumpeter, technological creative destruction drives long-term progress, even if it temporarily disrupts the labour market (Perihan, 2015).

---

14 It entails public trust and equality in ensuring that automation does not disproportionately benefit the wealthy at the expense of the everyday citizen.

15 Dizikes, P. (2022, December 21). Should we tax robots? MIT News. https://clck.ru/3QmUSe

16 Summers, L. (2017, March 5). Picking on Robots won't deal with Job Destruction. Washington Post (Washington DC). https://clck.ru/3QmUWe

3.2. Ambiguity in Defining what a robot is

Over the years since this debate, policymakers have struggled and are impasse on what constitutes robots, especially for taxation and liability purposes (Perihan, 2015). Questions arise on whether tax should apply to robotic industrial arms, physical humanoid machines replacing factory workers, AI software robots or basic software algorithms. Consequently, the EU's failed attempt at ascribing a definition to intelligent robots in its 2017 Liability Directive further deepens this ambiguity[17]. Enforcing a robot tax becomes unworkable without a clear legal or operational definition.

Hence, by these inconsistencies in classification, corporations are bound to manoeuvre these loopholes and regulatory arbitrage, as there is no absolute threshold in sight. Implementing any robot tax in this condition may become messy and prone to numerous abuses. Globally, countries already struggle with general tax compliance and policy enforcement (Monyake, 2023), and so introducing a robot tax could open the door to more corruption, confusion, mismanagement, bureaucratic complexities and loophole exploitation instead of streamlining tax governance. Furthermore, introducing robot taxes without foundational administrative capacity could lead to bureaucratic bottlenecks, policy misapplication and could be the exact opposite of what is intended for the public.

3.3. Risk of Capital Flight and Job Exportation

Owing to the competitive nature of the global market, corporations may choose to respond to new taxes by relocating to jurisdictions with favourable tax policies (Ossandón Cerda, 2020). Where they do stay, it could lead to higher prices of goods and services and companies that use robots may pass on the production cost of the tax to the customers in the form of higher prices, which could negatively impact household budgets. For instance, when the United States introduced tariffs on Chinese automation imports in 2019, manufacturers shifted operations to Vietnam[18]. Thus, a robot tax, if unilaterally applied, could accelerate capital flight and worsen job losses, especially in emerging economies that lack bargaining power in global markets. Furthermore, implementing a

[17] On 16 February 2017, the European Parliament voted on the recommendations made by the committee. However, it rejected the introduction of a statutory definition of robots, new corporate reporting requirements, and an advisory code of conduct for robotics engineers to guide the ethical design, production and use of robots because these measures could stifle innovation. Instead, it voted for a resolution calling upon the European Commission to propose legislation for a legal and ethical framework for robots and a debate on new employment models and the sustainability of tax and social security systems.

[18] Cyrill, M. (2019, January 24). Shifts in China's Industrial Supply Chain and the US-China Trade War. China Briefing. https://clck.ru/3QmUiq

robot tax can be viewed as a misdirected solution to a systemic flaw. The automation that robots bring only exposes deeper flaws in administrative systems and is not necessarily an inherent concern with the rise in technology per se.

A case analysis of South Korea shows that it granted a 3-7% tax credit to corporations that invest in automation and robots in 2017. Studies demonstrated that South Korean businesses increase employment and decrease their automation expenditure whenever the tax credit rate is lowered (Kang et al., 2024). The tax credit has had a positive fiscal externality, meaning that behavioural responses to tax credit reductions increased government revenue beyond the direct mechanical impact of the policy. The tax reform also decreased wage inequality by slowing wage growth in the upper half of the income distribution (Kang et al., 2024).

4. Localising the Debate: What then does this mean for Nigeria?

Taxation is not merely a tool for revenue generation but a moral and legal instrument for redistributing societal benefits and burdens. The Federal Inland Revenue Service in 2025 reported that its agency generated ₦21.6 trillion in revenue in 2024, exceeding its initial target of ₦19.4 trillion by 11.34%[19]. Moreover, the Nigerian financial sector generated a whopping ₦570.91 billion in corporate income tax in Q3 in 2024, a significant 21.5% of the total sums collected during that period[20]. The tax rate provided by the Tax Reform Act 2025 portrays the belief that wealth and responsibility should be shared in a fair and functioning society (Makar et al., 2025). Thus, taxing robots treats a symptom while ignoring the disease for a developing system like Nigeria and many African nations. This begs a critical question for diagnosis: Should a country like Nigeria focus its limited policy capital on taxing robots when the real need lies in building a fairer economic system that embodies inclusivity for all and is future-proof? At what point does innovation, while beneficial to firms and markets, become a form of exploitation, displacing workers somewhat without compensation, concentrating wealth in the hands of a few?

Unlike advanced countries where automation displaces millions of jobs, Nigeria's labour market remains informal, mainly low-skilled and unautomated. With many sectors still heavily relying on human labour, automation is not deeply embedded. As such, robot tax may be a misplaced policy attention attempting to solve a future problem while avoiding keen and urgent realities like poor digital infrastructure, low employability and

19 Federal Inland Revenue Service. Tax and Statistics Report: 2024 Statistics. https://goo.su/yLdKU

20 Ojoko, I. (2025, June 27). Nigeria's Financial Sector generates N570.91 billion in corporate income tax in Q3 2024, leading all sectors – Reports. Nairametrics. https://clck.ru/3QmUvp

tech literacy, high unemployment, informal sector dominance and weak legal labour protections.

More than ever, Nigeria should channel its impact on policies that build a resilient, just and humane economy. However, even though a full-fledged robot tax may not be viable for Nigeria now, its symbolic value should not be ignored. Thus, it signals a nation thinking proactively about the impact of automation and is willing to demand accountability and responsibility from tech-integrating industries. In other words, the proposition is a part of a broader fiscal reform strategy that reflects the values of equity, innovation and dignity through labour.

In essence, Nigeria's priorities must remain centred on restructuring the existing social contract (Ibrahim & Lanre, 2022) between the government and the citizens to ensure that their welfare and security are paramount. Hereon, growth must be human-centred, and innovations are ethical and inclusive, not merely exploitative in form (Singh et al., 2024). Technology must be seen as domestically empowering, not just imported. This would mean aligning labour, industry, taxation and education policies to collectively build an economy that can fully harness automation for the future of work without essentially leaving people behind. In the words of economist Mariana Mazzucato[21] innovation must be mission-driven; for Nigeria, the mission must be jobs, economic justice, ethics and shared prosperity.

Conclusion

The debate on whether the government should tax robots is intriguing and multifaceted, as it touches questions on equity, innovation, labour protection, and the state's role in shaping the future of work. Hence, this article has examined the arguments for and against taxing robots. It concludes that while robot taxation is not a universal remedy, when applied thoughtfully and contextually, it presents a strategic tool for navigating the impact of automation. In developed economies with advanced infrastructure and strong social safety nets, a robot tax can help mitigate job losses, redistribute gains from automation, and fund workers' retraining programmes without significantly stalling innovation.

However, for developing and underdeveloped nations like Nigeria, where automation is emergent and yet to reach critical mass, the urgent task lies in designing an inclusive, innovation-friendly economy anchored on digital infrastructure, job creation, and education reforms. In such a context, prematurely implementing a robot tax may hinder

[21] Mazzucato, M. (2018). Mission-Oriented Innovation Policy: Challenges and Opportunities. In SRIP Report 2018. https://clck.ru/3QmVEJ

growth and innovation at a critical stage of development. Therefore, governments must tailor their alternatives based on economic realities, embracing automation responsibly while prioritising equity and inclusive growth in meeting developmental goals. Global examples show that even advanced economies have shied away from direct robot taxation as of now. Robot taxation should not be viewed as an endpoint but instead as one of the many tools for managing the evolving relationship between humans, work, and machines in the 21st century. Ultimately, fiscal policy must evolve to capture value from technological gains and ensure that such gains lead to shared prosperity rather than deepening inequality. In so doing, Nigeria and other emerging economies can navigate the automation era with ambition and justice.

Based on the findings and conclusion from arguments for and against the debate of robot taxes, this paper proposes the following policy options for Nigeria to adopt.

1. Nigeria must reform its corporate tax codes to effectively and efficiently capture responsible automation gains. This strategy will also penalise future unjustified large-scale layoffs and encourage job-creating innovation. In addition, it will embed both legal, ethical and social considerations in Nigeria's digital economy policies and procurement frameworks. Specifically, the recent Tax Reform Law 2025, Companies and Allied Matters Act 2020, Corporate Affairs Commission's Regulations, the various Labour legislations and other future policies and regulations could be fine-tuned to contain these adjustments adequately.

2. Nigeria must establish a mandatory automation Impact assessment (AIAs). In this sense, for companies deploying large-scale automation, there will be a legal necessity to self-evaluate and disclose its impact on their current employees and wages. The AIA will visually explain the ensuing risks and offer workers a reconciliatory pathway.

3. Like South Korea, Nigeria may introduce incentive-based and modest levies on firms displacing workers through automation rather than punitive automation levies. Incentives to firms can include: tax breaks, grants or even soft loans to companies that retrain workers displaced by technology, create net employment through innovation or build local tech solutions or products. The levies can be allocated to create and fund national retraining and digital literacy programmes to produce a future-proof Nigerian workforce. Also, long-term strategies like labour market forecasting and youth entrepreneurship support will go a long way.

4. Finally, Nigeria can establish a multi-stakeholder policy forum to guide ethical automation and labour inclusion, involving public and private sector partnership made up of tech-savvy lawyers, AI researchers/ field experts, etc, academia and civil society groups.

References

Abbott, R., & Bogenschneider, B. (2018). Should Robots Pay Taxes? Tax Policy in the Age of Automation. *SSRN Electronic Journal*. 1659. https://doi.org/10.2139/ssrn.2932483

Adekanmbi, A., Olaoye, A., & Fakiyesi, O. A., (2024). An Empirical Analysis of Tax Revenue and Total Revenue of West African Countries. *International Journal of Business Management and Economic Review*, *7*(6). https://doi.org/10.35409/ijbmer.2024.3623

Carbonara, E., Parisi, M. L., & Pellegrino, G. (2024). Mitigating the labor displacing effects of automation: Robot taxes versus wage subsidies. *Journal of Evolutionary Economics*, *34*(1), 125–155. https://doi.org/10.1007/s00191-023-00826-4

Costinot, A., & Werning, I. (2022). Robots, trade, and Luddism: A sufficient statistic approach to optimal technology regulation. *Review of Economic Studies*, *89*(5), 2413–2448. https://doi.org/10.1093/restud/rdac018

Creighton, B., & McCrystal, Sh. (2016). Who is a Worker in International Law? *Comparative Labor Law and Policy Journal*, *37*(3), 691–725.

Dimitropoulou, Ch. (2024). *Robot Taxation A Normative Tax Policy Analysis – Domestic and International Tax Considerations*. IBFD Doctoral Series. https://doi.org/10.59403/cb75dv

Ibrahim, Ya., & Lanre, S. (2022). Social Contract Theory: A Model for Nation Building in Nigeria. *Journal of Administrative Science*, *9*(1), 136–154.

Gaus, A., & Hoxtell, W. (2019). Automation and the future of work in Sub-Saharan Africa. In *Automation and AI: Implications for African development prospects* (pp. 1–28). Center for Global Development. https://doi.org/10.2139/ssrn.3473564

Graetz, G., & Michaels, G. (2018). Robots at work. *Review of Economics and Statistics*, *100*(5), 753–768. https://doi.org/10.1162/rest_a_00754

Guerreiro, J., Rebelo, S., & Teles, P. (2023). Should robots be taxed? *American Economic Journal: Macroeconomics*, *15*(1), 1–38. https://doi.org/10.1257/mac.20200441

Kang, D., Lee, J. H., & Quach, S. (2024). The Welfare Effects of a Robot Tax: Evidence from a Tax Credit for Automation Technologies in Korea. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5005128

Kovacev, R. (2020). A Taxing Dilemma: Robot Taxes and the Challenges of Effective Taxation of AI, Automation and Robotics in the Fourth Industrial Revolution. *The Contemporary Tax Journal*, *9*(2), 4. https://doi.org/10.31979/2381-3679.2020.090204

Makar, D., Pilah, P., & Ayeh, R. (2025). New Tax Reforms 2025: You Earn, Spend, Buy, Sell, and Pay on Goods and Services already Taxed: A Comprehensive Analysis. *IRASS Journal of Economics and Business Management*, *2*(5), 10–24.

Mazur, O. (2019). Taxing the Robots. *Pepperdine Law Review*, *48*(2).

Mazur, O. (2024). The Taxation of Robots and Its Global Challenges. In S. V. Kostić et al. (Eds.), *Mobility of Individuals and Workforces*. https://doi.org/10.59403/2j0zh11019

Monyake, J. (2023). The Challenges of Managing Tax Compliance in Developing Countries: A Case of Botswana. *International Journal of Engineering Science Technologies*, *7*(6). https://doi.org/10.29121/ijoest.v7.i6.2023.551

Ossandón Cerda, F. (2020). Taxation on Robots? Challenges for Tax Policy in the Era of Automation. *Revista Chilena De Derecho Y Tecnología*, *9*(2), 187–219. (in Spanish). https://doi.org/10.5354/0719-2584.2020.55578

Perihan, H. K. (2015). Joseph A. Schumpeter's Perspective on Innovation. *International Journal of Economics, Commerce and Management*, *3*(8). https://ijecm.co.uk/wp-content/uploads/2015/08/383.pdf

Prettner, K., & Strulik, H. (2020). Technology, robots, and the future of work: A macroeconomic analysis. *Macroeconomic Dynamics*, *24*(5), 1153–1185.

Rayhan, A. (2023). *The Future Of Work: How AI and Automation will Transform Industries*. ResearchGate. https://doi.org/10.13140/RG.2.2.36092.51848

Singh, K., Chatterjee, Sh., & Mariani, M. (2024). Applications of Generative AI and the future of Organisational Performance: The Mediating Role of Explorative and Exploitative Innovation and Moderating Role of Ethical Dilemmas and Environmental Dynamism. *Technovation*, *133*, 103021. https://doi.org/10.1016/j.technovation.2024.103021

Thuemmel, U. (2023). Optimal taxation of robots. *Journal of the European Economic Association*, *21*(3), 1154–1190. https://doi.org/10.1093/jeea/jvac062

Zhang, P. (2019). Automation, wage inequality and implications of a robot tax. *Japan and the World Economy*, *51*, 1–13. https://doi.org/10.1016/j.japwor.2019.03.001

Zhang, P. (2021). You have been terminated: Robots, work, and taxation. *International Review of Economics & Finance*, *76*, 1020–1034. https://doi.org/10.1016/j.iref.2021.08.019

Author information

Deborah El. Otighi – LLB Bachelor of Laws, Redeemer's University
Address: P.M.B 230 Ede, Osun State, Nigeria
E-mail: otighi21668307@run.edu.ng
ORCID ID: https://orcid.org/0009-0007-8557-823X

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – July 31, 2025
Date of approval – August 13, 2025
Date of acceptance – December 20, 2025
Date of online placement – December 25, 2025

Научная статья
УДК 34:004:346.6:004.8:004.896:349.2
EDN: https://elibrary.ru/vluyug
DOI: https://doi.org/10.21202/jdtl.2025.28

Налогообложение робототехники как инструмент защиты рынка труда: правовой анализ перспектив для развивающихся экономик на примере Нигерии

Дебора Элохозино Отиги
Университет Искупителя, Эде, Нигерия

Ключевые слова

занятость,
искусственный интеллект,
налог,
налоговое право,
налогообложение,
право,
робототехника,
рынок труда,
трудовые отношения,
цифровые технологии

Аннотация

Цель комплексный правовой и экономический анализ обоснованности введения налога на робототехнику как меры защиты рынка труда в условиях нарастающей автоматизации с учетом социально-экономических реалий развивающейся экономики Нигерии.

Методы: исследование базируется на доктринальной и сравнительно-правовой методологии. Автор осуществляет системный анализ научных публикаций, законодательных актов, статистических данных и эмпирических материалов, касающихся влияния робототехники и искусственного интеллекта на глобальные рынки труда. Особое внимание уделяется изучению опыта налоговой политики в области автоматизации в Южной Корее и Европейском союзе, что позволяет выявить универсальные закономерности и специфические особенности регулирования автоматизации в различных юрисдикциях. Методологический инструментарий включает контент-анализ нормативных документов, экономико-статистический анализ данных международных организаций и критический анализ доктринальных позиций относительно перспектив налогообложения роботов.

Результаты: проведенное исследование демонстрирует неоднозначность института налогообложения робототехники в современной правовой и экономической системе. Выявлено, что налог на роботов потенциально способен замедлить темпы автоматизации, предоставить работникам время для адаптации и переквалификации, компенсировать сокращение поступлений подоходного налога и обеспечить экономическую справедливость путем перераспределения корпоративных доходов от автоматизации. Вместе с тем установлены существенные ограничения данной концепции: риск торможения инноваций, отсутствие единого юридического определения понятия «робот», угроза оттока капитала и смещения производств в юрисдикции

с более благоприятной налоговой средой. Применительно к Нигерии обоснован вывод о преждевременности введения налога на робототехнику в условиях низкого уровня автоматизации, высокой структурной безработицы, доминирования неформального сектора занятости и слабой цифровой инфраструктуры.

Научная новизна: работа представляет собой системное исследование правовых и экономических аспектов налогообложения робототехники применительно к правовой системе Нигерии. Новизна исследования состоит в обосновании контекстуального подхода к определению целесообразности введения налога на роботов с учетом стадии экономического развития, структуры рынка труда и степени проникновения технологий автоматизации. Автор впервые формулирует концепцию ответственной автоматизации для развивающихся экономик, предполагающую не карательное налогообложение, а стимулирующую систему мер, сочетающую умеренные сборы с инвестициями в человеческий капитал и цифровую инфраструктуру.

Практическая значимость: результаты исследования обладают высокой прикладной ценностью для формирования государственной политики в сфере регулирования автоматизации труда. Предложенные рекомендации – реформирование корпоративных налоговых кодексов с учетом ответственной автоматизации, введение обязательной оценки воздействия автоматизации на занятость, создание системы налоговых стимулов для компаний, переобучающих вытесненных технологиями работников, формирование многосторонней площадки по этическому управлению автоматизацией: могут быть использованы законодательными и исполнительными органами Нигерии и других развивающихся стран при разработке правовых механизмов регулирования цифровой экономики и защиты прав работников в условиях технологической трансформации.

Для цитирования

Отиги, Д. Э. (2025). Налогообложение робототехники как инструмент защиты рынка труда: правовой анализ перспектив для развивающихся экономик на примере Нигерии. *Journal of Digital Technologies and Law*, *3*(4), 705–721. https://doi.org/10.21202/jdtl.2025.28

Список литературы

Abbott, R., & Bogenschneider, B. (2018). Should Robots Pay Taxes? Tax Policy in the Age of Automation. *SSRN Electronic Journal*. 1659. https://doi.org/10.2139/ssrn.2932483

Adekanmbi, A., Olaoye, A., & Fakiyesi, O. A., (2024). An Empirical Analysis of Tax Revenue and Total Revenue of West African Countries. *International Journal of Business Management and Economic Review*, *7*(6). https://doi.org/10.35409/ijbmer.2024.3623

Carbonara, E., Parisi, M. L., & Pellegrino, G. (2024). Mitigating the labor displacing effects of automation: Robot taxes versus wage subsidies. *Journal of Evolutionary Economics*, *34*(1), 125–155. https://doi.org/10.1007/s00191-023-00826-4

Costinot, A., & Werning, I. (2022). Robots, trade, and Luddism: A sufficient statistic approach to optimal technology regulation. *Review of Economic Studies*, *89*(5), 2413–2448. https://doi.org/10.1093/restud/rdac018

Creighton, B., & McCrystal, Sh. (2016). Who is a Worker in International Law? *Comparative Labor Law and Policy Journal*, *37*(3), 691–725.

Dimitropoulou, Ch. (2024). *Robot Taxation A Normative Tax Policy Analysis – Domestic and International Tax Considerations*. IBFD Doctoral Series. https://doi.org/10.59403/cb75dv

Ibrahim, Ya., & Lanre, S. (2022). Social Contract Theory: A Model for Nation Building in Nigeria. *Journal of Administrative Science*, *9*(1), 136–154.

Gaus, A., & Hoxtell, W. (2019). Automation and the future of work in Sub-Saharan Africa. In *Automation and AI: Implications for African development prospects* (pp. 1–28). Center for Global Development. https://doi.org/10.2139/ssrn.3473564

Graetz, G., & Michaels, G. (2018). Robots at work. *Review of Economics and Statistics*, *100*(5), 753–768. https://doi.org/10.1162/rest_a_00754

Guerreiro, J., Rebelo, S., & Teles, P. (2023). Should robots be taxed? *American Economic Journal: Macroeconomics*, *15*(1), 1–38. https://doi.org/10.1257/mac.20200441

Kang, D., Lee, J. H., & Quach, S. (2024). The Welfare Effects of a Robot Tax: Evidence from a Tax Credit for Automation Technologies in Korea. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5005128

Kovacev, R. (2020). A Taxing Dilemma: Robot Taxes and the Challenges of Effective Taxation of AI, Automation and Robotics in the Fourth Industrial Revolution. *The Contemporary Tax Journal*, *9*(2), 4. https://doi.org/10.31979/2381-3679.2020.090204

Makar, D., Pilah, P., & Ayeh, R. (2025). New Tax Reforms 2025: You Earn, Spend, Buy, Sell, and Pay on Goods and Services already Taxed: A Comprehensive Analysis. *IRASS Journal of Economics and Business Management*, *2*(5), 10–24.

Mazur, O. (2019). Taxing the Robots. *Pepperdine Law Review*, *48*(2).

Mazur, O. (2024). The Taxation of Robots and Its Global Challenges. In S. V. Kostić et al. (Eds.), *Mobility of Individuals and Workforces*. https://doi.org/10.59403/2j0zh11019

Monyake, J. (2023). The Challenges of Managing Tax Compliance in Developing Countries: A Case of Botswana. *International Journal of Engineering Science Technologies*, *7*(6). https://doi.org/10.29121/ijoest.v7.i6.2023.551

Ossandón Cerda, F. (2020). Taxation on Robots? Challenges for Tax Policy in the Era of Automation. *Revista Chilena De Derecho Y Tecnología*, *9*(2), 187–219. (in Spanish). https://doi.org/10.5354/0719-2584.2020.55578

Perihan, H. K. (2015). Joseph A. Schumpeter's Perspective on Innovation. *International Journal of Economics, Commerce and Management*, *3*(8). https://ijecm.co.uk/wp-content/uploads/2015/08/383.pdf

Prettner, K., & Strulik, H. (2020). Technology, robots, and the future of work: A macroeconomic analysis. *Macroeconomic Dynamics*, *24*(5), 1153–1185.

Rayhan, A. (2023). *The Future Of Work: How AI and Automation will Transform Industries*. ResearchGate. https://doi.org/10.13140/RG.2.2.36092.51848

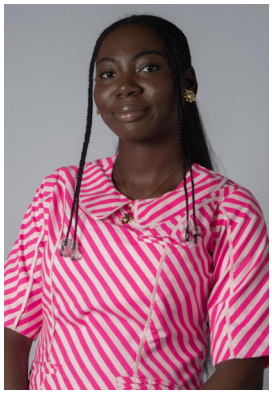
Singh, K., Chatterjee, Sh., & Mariani, M. (2024). Applications of Generative AI and the future of Organisational Performance: The Mediating Role of Explorative and Exploitative Innovation and Moderating Role of Ethical Dilemmas and Environmental Dynamism. *Technovation*, *133*, 103021. https://doi.org/10.1016/j.technovation.2024.103021

Thuemmel, U. (2023). Optimal taxation of robots. *Journal of the European Economic Association*, *21*(3), 1154–1190. https://doi.org/10.1093/jeea/jvac062

Zhang, P. (2019). Automation, wage inequality and implications of a robot tax. *Japan and the World Economy*, *51*, 1–13. https://doi.org/10.1016/j.japwor.2019.03.001

Zhang, P. (2021). You have been terminated: Robots, work, and taxation. *International Review of Economics & Finance*, *76*, 1020–1034. https://doi.org/10.1016/j.iref.2021.08.019

Сведения об авторе



Отиги Дебора Элохозино – бакалавр права, Университет Искупителя
Адрес: Нигерия, штат Осун, г. Эде, P.M.B 230
E-mail: otighi21668307@run.edu.ng
ORCID ID: https://orcid.org/0009-0007-8557-823X

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 31 июля 2025 г.
Дата одобрения после рецензирования – 13 августа 2025 г.
Дата принятия к опубликованию – 20 декабря 2025 г.
Дата онлайн-размещения – 25 декабря 2025 г.