PROTECTION OF HUMAN RIGHTS IN THE CONTEXT OF IMPLEMENTING ALGORITHMIC TECHNOLOGIES IN PRE-TRIAL INVESTIGATION

Kryvosheiev Mykola

DOI: https://doi.org/10.61345/1339-7915.2026.1.13

Annotation. This article provides a comprehensive and multi-layered analysis of the theoretical, legal, doctrinal, and ethical challenges determined by the systemic integration of algorithmic solutions and artificial intelligence (AI) technologies into the architecture of the modern criminal justice system. The author posits that the digital transformation of pre-trial investigation and judicial proceedings has catalyzed a fundamental ontological conflict between the paradigm of technological determinism – which prioritizes the maximization of procedural efficiency through the automated processing of vast datasets – and the classical anthropocentric legal paradigm, which asserts the absolute priority of fundamental human rights, individual agency, and personhood. This tension necessitates a radical re-evaluation of the conceptual foundations of criminal procedure in the era of the Fourth Industrial Revolution.

The research focuses on the epistemological risks inherent in the use of "black-box" algorithms within law enforcement, where the opacity of mathematical models utilized in predictive policing and recidivism risk assessment systems threatens the core principle of legal certainty. The author substantiates the necessity of a conceptual transition toward a new doctrine of "digital humanism." This doctrine is envisioned as a sophisticated synthesis of institutional legal safeguards and ethical engineering filters, implemented through the innovative framework of "Ethics by Design." It is argued that ethical norms must be embedded directly into technical protocols and the underlying source code of software utilized in criminal proceedings, thereby transforming algorithmic architecture into an accountable and transparent tool of justice rather than a self-governing entity.

A pivotal component of this study is the critical examination of the mathematical and socio-legal limitations of equity in automation. Specifically, the article explores the "Kleinberg-Chouldechova impossibility theorem of fairness," which demonstrates that different definitions of algorithmic equity – such as calibration, predictive parity, and error rate balance – are mathematically incompatible under certain conditions. The author argues that this theorem serves as a crucial warning against over-reliance on purely technical solutions to social bias. It underscores the fact that achieving "fairness" in a criminal justice context is not merely a computational task but a profound political and legal choice that requires human judgment to navigate the inherent trade-offs between competing metrics of equality.

Furthermore, the article addresses the transformative evolution of conventional human rights in the digital age. The author provides a detailed analysis of the genesis and substantive content of the "right to an explanation" regarding algorithmic logic, which is emerging as an indispensable condition for ensuring the right to a fair trial. It is demonstrated that without the ability of the defense to verify, challenge, and rebut algorithmic outputs, the adversarial character of the judicial process is fundamentally compromised. Additionally, the study investigates the persistent problem of algorithmic bias arising from the use of unrepresentative or historically skewed training data. The author asserts that protection against "automated stigmatization" must attain the status of a specialized procedural guarantee to prevent the perpetuation of systemic social prejudices through seemingly objective digital instruments.

In its concluding remarks, the article emphasizes that the legitimacy of innovative investigation and adjudication depends not on the technical perfection of algorithms, but on the legal system's capacity to ensure meaningful human oversight – the "human-in-the-loop" principle. The author concludes that the future of criminal procedural doctrine must focus on enhancing the transparency, explainability, and auditability of algorithmic systems. This study holds theoretical significance for the development of legal doctrine in the digital epoch and offers practical insights for the establishment of rigorous validation standards for forensic and investigative software, ensuring that technological progress serves the interests of truth and human dignity.

Key words: human rights, algorithmic technologies, pre-trial investigation, criminal law, digital humanism, artificial intelligence, algorithmic transparency, algorithmic bias, human-in-the-loop, black-box algorithms, ethics by design.

1. Introduction.

The accelerated integration of innovative technologies into criminal procedural activities gives rise to a fundamental dilemma between investigative efficiency and the protection of core human rights. Such technologies may simultaneously prove efficacious for crime detection and procedurally lawful, while remaining ethically untenable due to their potential to infringe upon human dignity, exert a chilling effect on democratic freedoms, or facilitate systemic discrimination against vulnerable populations. The theoretical and legal conceptualization of this issue is predicated on the necessity of balancing public interest (societal security) with private autonomy – a dynamic that acquires new ontological dimensions in the context of digital transformation.

A central challenge lies in the fact that classical criminal procedure concepts, established during the era of "material forensics," prove inadequate for regulating relations within the digital sphere. Specifically, a series of fundamental contradictions emerge:

1. The Crisis of Individual Autonomy: The mass collection of biometric data and the analysis of digital footprints (Big Data) effectively eliminate the "right to anonymity," transforming private life into an object of constant, proactive surveillance.

2. The Deficit of Algorithmic Transparency: The deployment of machine learning systems for risk assessment or identification precipitates the "black box" problem, wherein the logic underpinning procedurally significant decisions remains opaque to both the defense and the court, thereby undermining the principle of equality of arms.

3. The Blurring of Boundaries for Legitimate Interference: The transformation of evidence from physical objects into informational entities enables remote and imperceptible privacy intrusions, which complicates procedural oversight regarding the legality of investigative actions.

Given these considerations, scientific inquiry aimed at developing ethical filters and legal safeguards for "digital forensics" acquires profound relevance.

2. Analysis of scientific publications.

The legal and ethical challenges arising from the technologization of law enforcement constitute a complex, interdisciplinary field of inquiry. Notwithstanding the considerable interest in discrete aspects of technical and forensic support, a systemic analysis of the ethico-legal implications of this technological evolution is currently in its nascent stages of formation. Various facets of this problematic have been addressed by scholars such as P. Brey, A. Cavoukian, A. Chouldechova, S. Corbett-Davies, W. Fleisher, B. Friedman, P.K. Lin, and L. Zornetta, among others. An assessment of the current state of literature reveals a paucity of integrative research. The majority of existing scholarship remains focused on narrow, sector-specific issues – such as algorithmic bias or discrete ethical dilemmas – which precludes a comprehensive

elucidation of the broader systemic patterns governing the development of ethico-legal standards for technological application at the pre-trial investigation stage.

3. The aim of the work.

The objective of this study is to conduct a conceptual analysis and reconceptualize the substantive content of the categories of 'human rights,' 'privacy,' and 'ethics' in light of their transformation driven by the biotechnological and digital revolutions. Furthermore, the research aims to identify and systematize the risks inherent in the deployment of algorithmic methods within the framework of pre-trial investigations.

4. Review and discussion.

The implementation of innovative tools in pre-trial investigations is accompanied by a series of systemic legal risks that necessitate a revision of traditional procedural paradigms to ensure a balance between investigative efficiency and adherence to fundamental standards of justice. In modern criminal procedural doctrine, human rights should be viewed as a system of boundaries, defined by international and national law, which limit the coercive power of the state during the collection, processing, and application of forensically relevant information. The ultimate objective of such a system is the preservation of human dignity and liberty amidst the intensive digitalization of investigative activities.

In the era dominated by "digital forensics" and "genetic identification", a paradigmatic shift has occurred: human rights have expanded from the physical to the informational sphere. An evolutionary extension of these fundamental rights is "digital human rights" [1] – legal guarantees and standards predicated on human dignity that safeguard an individual's right to digital identity. This encompasses the right to the inviolability, uniqueness, and authenticity of one's digital profile – including biometric data, digital traces, and behavioral attributes – as well as the state's obligation to guarantee that this identity is not distorted, misappropriated, or erroneously interpreted by algorithmic systems. Furthermore, it includes the right to protection against unlawful interference in one's virtual environment, the guarantee of personal and biometric data security, and the right to a fair trial involving transparent and unbiased algorithmic systems.

Within the framework of pre-trial investigation, human rights function as a "legal filter" that determines the admissibility of evidence. Any technological innovation, such as mass facial recognition or Big Data analytics, must be subjected to a proportionality test. Currently, human rights, ethics, and transparency constitute the so-called "triangle of legitimacy" for forensic innovation. The absence of any of these elements renders a technology, regardless of its technical efficacy, unacceptable for integration into the legal system of a democratic state.

Accordingly, through the lens of forensic technologies, *human rights* can be defined as a system of fundamental guarantees protecting an individual's physical, digital, and biometric integrity from disproportionate or opaque interference. This system is operationalized through the rights to informational self-determination, the explainability of algorithmic decisions, and the adversarial scrutiny of technological evidence.

Conceptually, this definition is articulated through three core dimensions: 1. *Digital Privacy*; 2. *Algorithmic Fairness and Transparency*; and 3. *Human-Centricity* (*Human-in-the-Loop*).

1. Digital Privacy. The classical conception of the right to privacy, famously articulated by Warren and Brandeis in 1890 as the "right to be let alone" [2] and subsequently codified in international law (Article 12 of the Universal Declaration of Human Rights [3], Article 17 of the International Covenant on Civil and Political Rights [4], and Article 8 of the European Convention on Human Rights [5]) as protection against "arbitrary or unlawful interference" with one's private life, was rooted in a spatial paradigm. Within this framework, specific spheres of life (the home, correspondence, private documents) were designated as areas where an individual maintains a reasonable expectation of privacy, as opposed to public spaces where such an expectation is absent. This private-public dichotomy persisted in a world where surveillance was predominantly local, episodic, and necessitated the physical presence of an observer.

Contemporary pre-trial investigative technologies fundamentally disrupt this classical privacy paradigm through several key mechanisms:

– *Ubiquitous Surveillance:* The deployment of real-time automated facial recognition systems, geolocation data from mobile operators, and metadata regarding internet activity enables constant monitoring.

– *The Inferential Nature of Technology:* Machine learning algorithms go beyond recording observable behavior; they extrapolate latent information that an individual may never have explicitly disclosed, such as political affiliations, financial standing, medical conditions, or sexual orientation.

– *Data Vulnerability and Persistence:* Digital information can be instantaneously replicated, transferred across jurisdictions, stored indefinitely, or repurposed for objectives entirely divergent from the original intent.

– *The Proliferation of Biometric Collection:* Biometric data holds a qualitatively distinct status from other forms of personal information due to its uniqueness – biometric parameters serve as "lifelong identifiers" that cannot be altered – and its inferential potential (the ability to reveal sensitive information, such as ethnic origin or genetic predispositions). Consequently, the GDPR [6] and various national legal frameworks categorize biometric data as a "special category" of personal data requiring enhanced protection. Its processing is permitted only under specific conditions of consent or, in exceptional circumstances such as criminal investigations, subject to rigorous procedural safeguards.

Under contemporary conditions, the understanding of privacy is undergoing a profound transformation – shifting from the traditional "right to be let alone" toward the right to informational self-determination and the inviolability of personal and biometric data that can be identified, extracted, or analyzed via technical means. In the realm of forensic activity, privacy manifests through several interconnected dimensions:

Communicative and Digital Privacy: The inviolability of electronic traces, metadata, and correspondence, which are capable of reconstructing an individual's private life with a high degree of granularity (the concept of the "digital twin").

Biometric and Genetic Privacy: The protection of unique biological identifiers (such as DNA profiles), the processing of which by artificial intelligence algorithms constitutes a substantial interference with an individual's identity.

Spatial and Cognitive Privacy: Safeguards against covert remote surveillance, geolocation tracking, and predictive profiling methods aimed at identifying characteristic behavioral patterns without the individual's awareness.

From the perspective of forensic methodology, privacy at the pre-trial investigation stage functions as a normative regulator of technological invasiveness. It establishes the boundary at which the efficiency of an investigator's search-and-discovery activities must be subordinated to the principles of proportionality and necessity in a democratic society. Consequently, in the digital era, privacy evolves into a requirement for algorithmic accountability, technical transparency of the technologies used for evidentiary collection, and the principle of data minimization.

2. *Algorithmic Fairness and Transparency*. In the digital age, the substance of algorithmic fairness undergoes significant transformation, where ethics emerges as a foundational internal criterion for due process. Within this framework, the right to a fair trial is interpreted primarily as the right to audit and understand the algorithm.

The deployment of proprietary, "closed" software products ("black box" technologies) for DNA analysis, ballistic examinations, or risk assessments poses a direct threat to the transparency of justice. Legal protection, reinforced by the ethical imperative of transparency, dictates that every defendant must possess the right to know the underlying logic of the technology that identified them and must be granted a genuine procedural opportunity to challenge that logic.

Accordingly, ethics in forensic technologies is operationalized through the following dimensions:

Algorithmic Fairness: Ethics dictates that technology must not generate disproportionate risks for specific social or ethnic groups. This entails a rejection of predictive policing systems if they exhibit a bias toward discriminating against residents of particular neighborhoods or members of specific demographics. A technology is deemed ethical only when the probability of statistical error (False Positive/False Negative) is distributed equitably among all subjects, regardless of their status.

Protection from Algorithmic Discrimination: This dimension guarantees an individual's right to be evaluated based on their personal actions rather than the statistical profile of a group to which they belong. Predictive analytics technologies often carry the risk of labeling certain social or ethnic groups as "crime-prone." It is the state's duty to deploy only those systems that have undergone an independent bias audit.

Thus, ethics in forensic technologies constitutes a system of value standards and technical constraints ensuring that innovative methods (AI, biometrics, predictive analytics) are utilized in a manner that does not degrade human dignity, precludes algorithmic discrimination, and ensures the epistemic impartiality of truth-finding procedures.

The case of the COMPAS algorithm, developed by Northpointe, has become a seminal precedent in global scholarly discourse. The 2016 investigative report by *ProPublica* revealed systemic "algorithmic bias," manifested in a significantly higher probability of false-positive recidivism predictions for specific ethnic groups, thereby refuting claims regarding the axiological neutrality of artificial intelligence in the justice system.

The subsequent case of *State v. Loomis* [7] represented the judiciary's first attempt to legitimize AI while acknowledging its inherent limitations. In this instance, the defense for Loomis was denied the opportunity to scrutinize the algorithm's methodology, as it was protected under the developer's trade secrets. This case highlighted the "*black box*" problem, where the proprietary nature of the technology precludes a technical audit of the methodology by the defense, effectively nullifying the principles of transparency and the equality of arms.

The *State v. Loomis* case established the theoretical groundwork for the transition toward the paradigm of *Explainable Artificial Intelligence (XAI)* and the requirement of *algorithmic transparency*. This is defined as the state of accessibility, intelligibility, and verifiability of the logical and technical processes governing an innovative system, ensuring that parties to criminal proceedings and the court can scrutinize the reliability, accuracy, and impartiality of the generated outputs.

3. Human-centricity (Human-in-the-Loop) refers to the fundamental right of an individual to ensure that any final decision significantly impacting their liberty – such as a notice of suspicion or a motion for detention – is made exclusively by a human agent (an investigator, prosecutor, or judge) rather than an automated system. Technology must serve solely as an auxiliary tool, never as the ultimate arbiter. This anthropocentric approach necessitates a shift from passive reaction toward technological risks to the proactive implementation of the **"***Values by Design*" paradigm. This involves embedding *Privacy by Design* and *Ethics by Design* standards directly into the digital architecture. In synergy with the concept of *Explainable AI (XAI)*, this approach ensures the transparency of algorithmic determinations.

The outlined transformation of the substantive content of human rights amidst intensive technological advancement reshapes the principles of pre-trial investigation and creates an urgent need for an updated theoretical and doctrinal framework for forensic technology. The future development of a legal regulatory strategy for innovation must be based on a philosophical-legal synthesis, where classical legal principles of proportionality and subsidiarity are organically integrated with the nascent concept of digital humanism.

The theoretical conceptualization of the contemporary innovative transformation of pre-trial investigation is rooted in several fundamental concepts, the most vital of which is *digital humanism* [8]. This approach is predicated on the priority of human dignity and human rights over technological expediency. A critical extension of this is the human-in-the-loop approach, which substantiates the necessity of maintaining final

human control (by the investigator or expert) over algorithmic decisions. This ensures legal accountability and prevents "algorithmic determinism," a state wherein mathematical logic supplants the procedural inner conviction of the subject of proof.

An analysis of the legal and ethical challenges posed by innovative technologies in pre-trial investigations demonstrates the inadequacy of the reactive regulatory model, wherein the law attempts to "catch up" with technological advancement *post-factum*. An alternative to this model is the "Values by Design" or "Privacy by Design" paradigm. Under this approach, regulatory requirements – including privacy protection, bias mitigation, transparency, and accountability – must be integrated into the very architecture of the technology during the development phase, rather than being appended as an afterthought.

The concepts of "Values by Design," "Privacy by Design," and "Ethics by Design" (EbD) represent a paradigmatic shift in the methodology of developing and deploying forensic technologies. They necessitate the direct integration of ethical values, legal constraints, and human rights standards into the architecture (algorithm, code, and design) of a technical tool at the stage of its conceptualization. EbD constitutes an evolutionary extension of the "Privacy by Design" concept (pioneered by Ann Cavoukian in the 1990s) [9], yet it possesses a significantly broader regulatory scope.

EbD is underpinned by the theory of "Value Sensitive Design" (VSD), which posits that technology is not axiologically neutral; rather, it inherently embodies the values and biases of its creators. In a forensic context, this implies that an algorithm that fails to incorporate the presumption of innocence "at the level of the code" is fundamentally legally defective.

The implementation of the Ethics by Design (EbD) concept necessitates adherence to five foundational principles:

1. Algorithmic Transparency and Explainability: The technology must be engineered such that its conclusions are interpretable by a human agent (investigator, judge, or defense counsel). The utilization of Explainable AI (XAI) methods circumvents the "black box" problem, ensuring that the logic underpinning evidentiary formation is accessible for technical and legal audit.

2. Automated Data Minimization: The system must be programmed to automatically delete or mask redundant information irrelevant to the scope of the investigation. A practical application includes the automated blurring of faces of random bystanders in video footage who are not subjects of the search.

3. Bias Mitigation: During the algorithmic training phase (e.g., for facial recognition systems), representative datasets must be utilized to eliminate the risk of discrimination based on racial, ethnic, or gender characteristics.

4. Auditability: The system architecture must provide for the automatic logging of all operations, enabling the reconstruction of the provenance of each individual piece of evidence to ensure its procedural legitimacy and admissibility.

5. Human-in-the-Loop: The design of innovative tools must technically preclude the autonomous formulation of procedural decisions by a machine. The system's role is strictly confined to decision support, while ultimate legal responsibility remains with the investigator.

The "Ethics by Design" concept serves as the primary mechanism for preserving democratic standards of justice amidst the increasing **"**algorithmization" of crime and investigation. It facilitates a critical shift from a reactive regulatory model to a proactive one, characterized by the preventive exclusion of human rights violations through technical means.

The case of *State v. Loomis* underscored the necessity for research regarding the theoretical substantiation of algorithmic fairness, shifting the discourse from the realm of purely procedural safeguards to the spheres of mathematical ethics and epistemology. According to the *"Impossibility Theorem of Fairness"* formulated by Kleinberg and Chouldechova [10, 11], mathematical models are incapable of simultaneously ensuring

parity across all algorithmic fairness metrics. In the context of law enforcement, this limitation may result in the biased profiling of vulnerable populations (manifesting as racism, sexism, ableism, and other forms of discrimination). The theorem highlights the inherent mathematical constraints of algorithms and substantiates the necessity of making an *ethical choice* between competing models of fairness when configuring forensic systems.

The essence of this theorem lies in the proven mathematical incompatibility of three fundamental criteria of algorithmic fairness: statistical parity (equalized odds), calibration, and predictive parity (error rate balance). The authors mathematically demonstrated that in scenarios where base rates of a phenomenon differ across various population groups (e.g., based on ethnic or social characteristics), an algorithm is mathematically unable to satisfy all three fairness requirements simultaneously.

The theorem demonstrates that prioritizing one fairness criterion (such as ensuring an equal probability of false arrests across different groups) inevitably results in the violation of another (such as a disparity in predictive accuracy for those same groups). Consequently, the "Impossibility Theorem of Fairness" recontextualizes the problem of algorithmic bias from a purely technical dimension into a *politico-legal* one. It asserts that "fairness" cannot be achieved solely through code optimization; rather, it requires a conscious choice by society and the legislator regarding which type of algorithmic accuracy may be sacrificed to achieve a specific social good.

The mathematical limitations identified in the theorem are not a death knell for algorithmic fairness; instead, they emphasize that its realization is less a matter of code and more a question of political strategy and legal regulation aimed at balancing conflicting social interests. The mathematical contradiction among fairness criteria compels the abandonment of the illusion of "technological neutrality" in favor of a model of conscious trade-offs. In criminal proceedings, this necessitates a legal answer to a critical question: is it permissible to sacrifice the overall accuracy of a system to eliminate discriminatory disproportionality in false positives regarding vulnerable groups [12]?

Balancing competing interests – efficiency, accuracy, equality, and justice – always entails a *compromise* [13]. Given the mathematical proof of the "Impossibility Theorem of Fairness," according to which the simultaneous achievement of all parameters of statistical accuracy and equality is impossible, the law enforcement system must transition to a strategy of overtly declaring the value-based criteria embedded within each specific software tool. This transparency should be grounded in four key priorities that define the legitimacy of using innovations in the process of proving.

The first and foundational priority is transparency, realized through the implementation of the *"Right to Explanation".* This model shifts the emphasis from the final outcome to the quality of the procedure itself. According to this approach, an algorithm whose internal logic remains opaque cannot be integrated into the criminal process, regardless of its technical accuracy metrics. The critical factor for criminal proceedings here is not the mere fact of an AI-generated conclusion, but the existence of a genuine opportunity for the suspect to understand the stages of the system's cognitive analysis and to challenge them effectively within an adversarial process. The concept of *Explainable AI (XAI)* dictates that the results of automated data processing must be interpretable and intelligible to all participants in the investigation. Implementing this approach is vital for ensuring the right to a fair trial, as only an explainable algorithm enables the principle of equality of arms and provides the defense with the means to verify the reliability of evidence.

The priority of *Equalized Odds*, which involves the mathematical equalization of false identification rates to prevent systemic bias, requires developers and law enforcement agencies to ensure – specifically in the context of Automated Facial Recognition Technology (FRT) – that the algorithm does not produce *False Positives* for members of particular ethnic or social groups more frequently than for others. To prevent discrimination, it is considered permissible to deliberately reduce the overall predictive accuracy of a system if such a trade-off is necessary to achieve an identical rate of false accusations across all demographic groups.

Conversely, the priority of *Predictive Accuracy* focuses on maximizing the efficiency of truth-finding. Under this model, an algorithm that identifies a perpetrator in the vast majority of cases is deemed "fair" from

the perspective of the goals of criminal proceedings regarding swift and comprehensive investigation. However, such a model carries inherent risks of "technocratic determinism" and thus requires mitigation through the priority of human oversight – the *"Human-in-the-loop" principle*. The latter establishes the *subsidiary nature* of algorithmic systems, defining them as intellectual support tools rather than autonomous decision-making entities. The subject of the proceedings is obligated to conduct an independent cognitive verification of the system's logic, evaluating the generated data in conjunction with the totality of other evidence.

5. Conclusions.

This study establishes that the integration of innovative technologies into forensic activities during the pre-trial investigation stage has precipitated a fundamental shift in the legal paradigm: moving from the traditional protection of physical integrity toward the safeguarding of *informational self-determination* and *digital human rights*. It has been determined that the primary contemporary challenge lies in resolving the contradiction between technological determinism, which seeks maximum investigative efficiency, and the anthropocentric approach, which demands unconditional adherence to fundamental human rights.

The systemic ethicality of innovations is ensured through the implementation of the *Ethics by Design* principle and the *Human-in-the-Loop* model, wherein technology remains a subsidiary tool of intellectual support. This approach necessitates the integration of ethical filters and data minimization mechanisms directly into the system architecture during the development phase. Consequently, abandoning "proprietary" closed algorithms in favor of transparent methodologies is a prerequisite for ensuring institutional trust in forensic investigation outcomes within a democratic society.

The theoretical-legal foundation of this research confirms that phenomena such as the "black box effect" and algorithmic bias are not merely technical defects but possess deep axiological roots. Drawing upon the Kleinberg-Chouldechova impossibility theorem of fairness, it is demonstrated that the selection of an algorithm's mathematical model is an ethico-legal decision requiring state regulation. Thus, the concepts of *Ethics by Design* and Explainable AI (XAI) must be regarded not as optional recommendations but as imperative requirements for the architecture of forensic systems. Epistemological transparency and explainability emerge as imperatives under which a developer's trade secret cannot restrict the defense's right to verify the underlying logic of generated results and system error rates.

In conclusion, the emergence of a new theoretical-legal paradigm – *"Digital Humanism"* in criminal proceedings – can be observed. Within the framework of digital humanism, innovative technologies serve as instruments for enhancing human cognitive capacity, provided that the moral integrity of the process is preserved. This model offers a resolution to the central dilemma of the modern era: how to utilize the unprecedented power of artificial intelligence without transforming the criminal process into a mere algorithmic calculation devoid of ethical substance.

References:

1. Walshe, P. (2020). Digital identity: Report prepared for the Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (T-PD(2020)04rev). Council of Europe. https://rm.coe.int/t-pd-2020-04rev-digital-identity-tc-en/1680a0c051

2. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220. https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

3. UN General Assembly. (1948). Universal declaration of human rights (217 A (III)). https://www.un.org/en/about-us/universal-declaration-of-human-rights

4. UN General Assembly. (1966). International covenant on civil and political rights (United Nations Treaty Series, Vol. 999, p. 171). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

5. Council of Europe. (1950). European convention for the protection of human rights and fundamental freedoms, as amended by Protocols Nos. 11 and 14 (ETS No. 5). https://www.echr.coe.int/documents/convention_eng.pdf

6. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

7. Supreme Court of Wisconsin. (2016). State v. Loomis, 881 N.W.2d 749. https://www.wicourts.gov/sc/opinion/DisplayDocument.pdf?content=pdf&seqNo=171690

8. Nida-Rümelin, J., & Weidenfeld, N. (2022). Digital humanism: For a humane transformation of democracy, economy and culture in the digital age. Springer. https://doi.org/10.1007/978-3-031-12482-2

9. Cavoukian, A. (2009). Privacy by design. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/en/media/1826/download?attachment

10. Kleinberg, J., Mullainathan, S., & Raghavan, M. (2016). Inherent trade-offs in the fair determination of risk scores. Proceedings of the 8th Innovations in Theoretical Computer Science Conference (ITCS 2017). https://arxiv.org/abs/1609.05807

11. Chouldechova, A. (2017). Fair prediction with disparate impact: A study of bias in recidivism prediction instruments. Big Data, 5(2), 153–163. https://doi.org/10.1089/big.2016.0047

12. Corbet-Davies, S., Pierson, E., Feller, A., Goel, S., & Huq, A. (2017). Algorithmic decision making and the cost of fairness. Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '17), 797–806. https://doi.org/10.1145/3097983.3098095

13. Lin, P. K. (2021). Machine see, machine do: How technology mirrors bias in our criminal justice system. New Degree Press.

Mykola Kryvosheiev,
postgraduate, Department of Law, P.H.E.I. «European University»
Kyiv, Ukraine
E-mail: kryvosheev@e-u.edu.ua
ORCID: 0009-0004-7414-4944