

PROTECTION OF THE COGNITIVE AND DIGITAL INTEGRITY OF THE INDIVIDUAL

Kravchuk S. M.

INTRODUCTION

The rapid development of artificial intelligence technologies (hereinafter – AI), machine learning, neuromodulation, and brain-computer interfaces in the third decade of the twenty-first century has led to an unprecedented shift in the paradigm of human rights and the system of social values. Whereas historically criminal law was formed around the protection of physical integrity, property, and public order, today the epicenter of socially dangerous encroachments is shifting into the neuro-digital continuum. Modern individuals find themselves in the conditions of “surveillance capitalism,” where their behavioral patterns, emotions, worldview orientations, and even neurobiological reactions become objects of collection, analysis, and commercial or political exploitation. This generates new existential threats related to the manipulation of choice, distortion of identity, and unauthorized access to the mental sphere of the individual.

Particularly acute is the problem of the proliferation of deepfake technologies and algorithmic manipulation, which erode the boundary between reality and simulacrum, causing irreparable harm to an individual’s reputation and mental well-being. Under such conditions, there arises an urgent need to formulate a new legal doctrine – that of “digital dignity,” which would guarantee protection of the subject from depersonalization within the virtual environment. At the same time, the emergence of commercial neuro-gadgets brings to the forefront the issue of protecting neuro-rights (freedom of thought, mental integrity), which has already found reflection in the first precedents of constitutional regulation worldwide (for example, in the Republic of Chile) and in international declarations of the Council of Europe.

However, criminal-law doctrine significantly lags behind technological progress. Traditional elements of criminal offenses do not encompass the specific nature of encroachments upon cognitive autonomy and free will under conditions of algorithmic determinism. The adoption of Regulation (EU) 2024/1689 of the European Parliament and of the Council (AI Act¹), which establishes prohibitions on the use of AI for subconscious manipulation, constitutes only the first step toward the formation of a global security architecture. Ensuring cognitive and digital integrity requires a profound theoretical reconsideration of the object of criminal-law protection and the definition of clear boundaries for the criminalization of emerging acts such as “neurohacking” or algorithmic coercion. Accordingly, the study of the

¹ Регламент Європейського Парламенту та Ради (ЄС) 2024/1689 щодо встановлення гармонізованих правил щодо штучного інтелекту (AI Act). *Офіційний вісник Європейського Союзу*, 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 12.03.2026).

theoretical and legal foundations for the protection of the cognitive and digital integrity of the individual acquires exceptional scientific and practical relevance.

The purpose of the research is to develop a comprehensive theoretical and legal concept of criminal-law protection of the cognitive and digital integrity of the individual under conditions of global digitalization, the algorithmization of social processes, and the development of neurotechnologies, as well as to formulate scientifically substantiated proposals for the modernization of criminal legislation.

Research objectives. In order to achieve the stated purpose, the following key objectives have been defined:

1. To conceptualize the notions of “neuro-rights,” “cognitive freedom,” and “mental integrity” as emerging objects of criminal-law protection.

2. To determine the theoretical foundations and criteria for the criminalization of unauthorized interference with human brain activity (“neurohacking”) and the use of neurotechnologies for unlawful purposes.

3. To examine the evolution of the concept of dignity in cyberspace and to formulate the doctrine of “digital dignity” as an autonomous legal value requiring protection against deepfakes and digital identity theft.

4. To analyze the level of social danger posed by algorithmic manipulation of consciousness and to distinguish aggressive algorithmic marketing from criminally punishable encroachments upon individual autonomy.

5. To reveal the ontological content of the “right to non-algorithmic existence” and to substantiate mechanisms for counteracting algorithmic determinism.

6. To develop prospective models for the implementation of international standards for the protection of the mental and digital sphere (in particular, on the basis of the provisions of the European AI Act) into national criminal legislation.

Object of the research – social relations arising in the sphere of ensuring, exercising, and legally protecting the fundamental human rights to mental, cognitive, and digital inviolability in the conditions of the information society and the development of artificial intelligence.

Subject of the research – theoretical and legal concepts of criminal law, doctrinal approaches to the understanding of digital dignity and neuro-rights, norms of international and national law regulating the protection of cognitive and digital integrity, as well as forms of socially dangerous encroachments in this sphere (neurohacking, algorithmic manipulation, and the creation of deepfakes).

Research methods. The methodological foundation of the research is formed by a comprehensive system of general scientific and specialized legal methods of inquiry, the selection of which is determined by the specific nature of the object, subject, purpose, and objectives of the study.

The dialectical method was applied to examine the evolution of human rights in the context of technological progress, which made it possible to trace the transition from the protection of exclusively physical integrity to the necessity of safeguarding the digital and cognitive sphere of the individual.

Methods of analysis and synthesis were employed to deconstruct complex technological phenomena (such as deepfakes and algorithmic manipulation) into their individual structural elements, followed by the synthesis of new criminal-law categories and the assessment of their level of social danger.

The structural-functional method makes it possible to determine the place and role of neurotechnologies and artificial intelligence systems within the system of contemporary social risks, as well as to evaluate the effectiveness of the existing functions of criminal law in responding to these challenges.

The hermeneutic method is applied to interpret the content of emerging legal concepts, international legal instruments (in particular the EU Regulation on AI), and doctrinal concepts in the field of neuroethics.

The dogmatic (formal-legal) method serves as a tool for the critical analysis of existing provisions of criminal legislation with the aim of identifying legal gaps concerning the qualification of encroachments upon digital dignity and developing proposals for improving the dispositions of criminal-law norms.

The comparative-legal method was used to study advanced foreign experience in the field of protecting neuro-rights and cognitive autonomy.

1. Criminal Law Protection of Human Neurorights (Theoretical Foundations for the Criminalization of Interference into the Mental Sphere)

1.1. Conceptualization of neuro-rights: freedom of thought, cognitive freedom, and mental integrity in the paradigm of the twenty-first century

The fundamental doctrine of criminal law throughout its historical development has been constructed around the presumption of the inviolability of the human body and the protection of material goods. The mental sphere, processes of thinking, and the formation of will have traditionally been regarded as *res extra commercium* (things withdrawn from circulation) and as a kind of “citadel” inaccessible to direct physical or technological interference from the outside. However, the transition to an information society and the unprecedented progress in the field of neuroscience have fundamentally transformed this paradigm. Contemporary criminal law of the postmodern era faces a challenge in which the human brain ceases to be solely a biological organ and becomes an informational node capable of direct interaction with digital networks, which requires the immediate conceptualization of new objects of criminal-law protection².

A response to this technological challenge has been the emergence of the concept of “neuro-rights” (neurorights) – a system of specific human rights aimed at protecting the brain and consciousness from unauthorized interference. Leading researchers in the field of neuroethics identify cognitive freedom as a fundamental, generic legal value that serves as the foundation for all other neuro-rights. Cognitive freedom possesses a dual nature: on the one hand (the negative aspect), it represents the absolute right of an individual to protection from coercive or covert interference in mental processes; on the other hand (the positive aspect), it constitutes the right to free access to neurotechnologies for the enhancement of one’s own cognitive capacities. From the perspective of criminal law, an encroachment upon the negative aspect of cognitive freedom represents an exceptionally high level of social danger,

² Радутний О. Е. Кримінально-правовий вимір штучного інтелекту та нейротехнологій. *Право та інновації*. 2021. № 1. С. 56–63.

as it undermines the very foundation of criminal liability – the freedom of will of the individual.

A key element of the system of neuro-rights is the right to mental integrity³. Unlike the traditional understanding of psychological integrity, which protects a person from psychological violence (threats, blackmail, abuse), mental integrity in the digital age focuses on protection against hardware and software interference with neurobiological and synaptic processes. From the standpoint of criminal law, such interference does not fall under the classical features of bodily injury, since it may leave no physical traces in brain tissue, yet it is capable of fundamentally altering the manner and content of an individual's decision-making⁴, inducing artificial emotions, or erasing portions of memory.

Another critically important object of protection is the psychological continuity (identity) of the individual. The use of deep brain stimulation (DBS) or the implantation of microchips creates a phenomenon in which a person may lose the ability to distinguish their own thoughts from those generated or modified by an algorithm. Criminal encroachment upon psychological continuity constitutes a form of “identity theft” at the highest level, where the very core of the human “self” is destroyed. This requires legislators to construct new elements of criminal offenses⁵, in which the consequence is recognized not as material damage or physical pain, but as the loss of the subject's authenticity.

Comparative legal analysis indicates that the international community has already begun the process of legalizing neuro-rights. A pioneering example in this direction is the experience of the Republic of Chile. In 2021, Chile became the first country in the world to amend its Constitution (Article 19), explicitly enshrining the protection of brain activity and the information derived from it. In further development of this provision, a separate law was adopted establishing strict limitations on the use of neurotechnologies and equating neurodata with medical data of the highest level of confidentiality, prohibiting their purchase and sale⁶. Such legislative innovation demonstrates that the criminalization of encroachments upon neuro-rights is not a hypothetical prospect but an urgent necessity of the present time.

The Declaration on the Protection of Neuro-rights in the Digital Age should recognize mental integrity. Its purpose is to establish ethical and legal boundaries aimed at protecting mental privacy, cognitive freedom, and brain data from abuse by neurotechnologies and artificial intelligence. It should set out fundamental guidelines for national governments. The document should also emphasize the necessity of adapting criminal and civil legislation to the risks of unauthorized decoding of thoughts and covert neuromodulation. The formation of an international legal consensus around neuro-rights will create a solid foundation for the implementation

³ Гуторова Н. О. Ментальна недоторканність як об'єкт кримінально-правової охорони у цифрову епоху. Вісник Асоціації кримінального права. 2022. № 1. С. 120–129.

⁴ Туляков В. О. Кримінальне право постмодерну та виклики алгоритмізації. *Слово Національної школи суддів*. 2022. № 3. С. 45–52.

⁵ Барабаш Ю. Г. Цифрова гідність: конституційно-правовий та кримінальний аспекти. *Право України*. 2023. № 2. С. 89–97.

⁶ Наїф аль Родхан Нейротехнології та нейроправа. URL: <https://zbruc.eu/node/105492> (дата звернення: 12.03.2026).

of relevant norms in the national criminal legislation of European states, including Ukraine.

1.2. Neurotechnologies (neuromodulation, brain–computer interfaces) as a novel object and subject of criminal-law protection

Brain-computer interfaces (BCI)⁷ constitute a key technological substrate enabling direct communication between the human central nervous system and external computing devices. According to their functional orientation, BCIs are divided into one-directional systems (either only reading neural signals or only stimulating them) and bidirectional systems (capable of simultaneously analyzing brain states and exerting feedback influence). The transition of these technologies from purely clinical medicine (where they were used to treat epilepsy or Parkinson's disease) into the sphere of commercial consumption (gaming, neuromarketing, the military sector) has resulted in a geometric growth of criminogenic risks.

In the context of criminal law, it is critically important to determine the legal nature of “brain data” (neurodata) circulating through BCIs. Neurodata fundamentally differs from traditional biometrics (fingerprints, DNA, retinal scans). While classical biometrics merely allows the identification of a person, neurodata makes it possible to decode their internal state: emotions, levels of concentration, hidden preferences, and even subconscious reactions to particular stimuli. Accordingly, neurodata constitutes a unique object of criminal encroachment, the unlawful acquisition of which represents a violation of mental privacy.

Doctrinal discussions concerning the status of neurodata⁸ revolve around the problem of their legal qualification. Should they be regarded as a form of information with restricted access, or should they instead be considered an inseparable part of the biological body of a person (a digital extension of the personality)? If the latter approach is adopted, then the unauthorized extraction of neurodata should be classified not merely as a computer crime but as a crime against the person, akin to the unlawful removal of organs or tissues. Such an approach requires a fundamental reconsideration of the object of criminal offenses in the sphere of computer systems, shifting the focus from the protection of information and telecommunication systems to the protection of the bio-digital integrity of the individual.

An even greater level of social danger is posed by the use of active neuromodulation technologies⁹ (for example, transcranial magnetic stimulation – TMS, or transcranial direct current stimulation – tDCS) as an instrument for committing crimes. Such technologies allow targeted influence on specific areas of the cerebral cortex by suppressing or stimulating particular neural ensembles. An

⁷ Нестеренко О. В., Яцук П. П. III (не) проти III. *Екологічна безпека та природокористування*. 2025. Вип. 4 (56). С. 134–153. URI: <http://e.ieu.edu.ua/handle/123456789/1414> (дата звернення: 12.03.2026).

⁸ Шевцов А. Г. Критичний аналіз поняття «свідомості» в сучасній методології штучного інтелекту. *Технології розвитку інтелекту*. 2025. Т. 9, № 1 (37). С. 1–22. DOI: <https://doi.org/10.31108/3.2025.9.7>

⁹ Орловський М. С., Іващенко С. М. Мультимодальні реабілітаційні стратегії у подоланні фантомного болю: огляд інноваційних практик та перспективи розвитку. *Неврологія*. 2025. С. 89–97. DOI: <https://doi.org/10.31640/LS-2026-1-10>

offender who gains access to a victim's BCI could remotely induce a state of acute pain, a panic attack, euphoria, or extreme aggression. In such cases, neurotechnology becomes a high-tech instrument of physical or psychological violence that leaves no traditional traces at the crime scene.

Legal regulation of these issues at the international level is only beginning to emerge. The adopted AI Act prohibits the use of AI systems that employ subliminal techniques or exploit the vulnerabilities of individuals in order to substantially distort their behavior in ways that may cause physical or psychological harm. However, the AI Act is regulatory rather than criminal in nature. It establishes administrative fines for corporations but does not address the issue of criminal liability for specific individuals who intentionally use neuromodulation to inflict harm. This creates what may be termed a "regulatory gap," where conduct is recognized as unlawful at the level of public law but has not yet been accompanied by an adequate criminal-law prohibition.

Thus, within criminal law neurotechnologies acquire a complex dual nature. On the one hand, they constitute a vulnerable object and subject of cyber-encroachments (when the software of an implant is hacked or neurodata is stolen); on the other hand, they become a powerful and covert instrument of manipulation and harm. This requires the science of criminal law to develop new conceptual approaches to understanding the instruments and means of committing crimes in the era of convergence between biological and digital systems.

1.3. Theoretical foundations for the criminalization of "neurohacking" and unauthorized interference with brain activity: challenges for the doctrine of criminal law

The process of conceptualizing the social danger of interference in the mental sphere inevitably leads to the necessity of developing a theoretical model for the criminalization of such conduct, which in scholarly discourse has been termed "neurohacking" (neurohacking)¹⁰. In a broad sense, neurohacking is defined as any intentional, unauthorized interference with the functioning of neuro-computer systems carried out with the aim of unlawfully intercepting, destroying, or modifying neurodata, or of seizing control over an individual's cognitive or motor functions. The challenges that neurohacking poses to the doctrine of criminal law are unprecedented, as they affect the fundamental constructions of the elements of a criminal offense.

The construction of the objective element (*actus reus*) of neurohacking requires moving beyond the existing norms governing cybercrime. Researchers propose differentiating the objective element into two independent forms. The first form is "cognitive espionage" (passive neurohacking), which consists in the covert reading of neural signals without the individual's consent (for example, through hacking a consumer neuro-headset in order to extract banking passwords or political preferences while the user views content in virtual reality). The second form is "neuromodulatory sabotage" (active neurohacking), which involves the forced alteration of neural activity (the writing of information into the brain) that leads

¹⁰ Ienca M., Scheibner J. Chapter Eight – What is neurohacking? *Defining the conceptual, ethical and legal boundaries*. 2020. Vol. 3. DOI: <https://doi.org/10.1016/bs.dnb.2020.03.008>

to changes in emotional states, beliefs, or the inducement of particular actions. Active neurohacking constitutes the most severe form of encroachment upon personal autonomy and should be subject to the strictest penalties¹¹.

The issue of establishing the subjective element (*mens rea*) in the investigation of such cases is extraordinarily complex. The specificity of neurotechnologies lies in the fact that they are often governed by machine-learning algorithms characterized by the so-called “black box problem.” This means that even the developer may not be able to precisely predict how the algorithm will interpret or modify the neural signal of a particular user. Accordingly, proving direct intent to cause mental harm becomes a nontrivial task. Investigators will have to distinguish between situations in which a change in psychological state occurred as a result of a technical malfunction (negligence), a side effect of a lawful algorithm (accident), or as the consequence of a deliberate criminal intention on the part of a hacker or corporation.

A separate doctrinal challenge concerns the establishment of a causal link between the act of neurohacking and its consequences, particularly in the context of induced criminal behavior. Consider the following scenario: an offender hacks the victim’s medical neuroimplant and induces a state of uncontrollable aggression, as a result of which the victim inflicts grievous bodily harm upon a third person. The question arises whether the victim should bear criminal liability. From the standpoint of classical criminal law, this situation contains elements of irresistible physical and psychological coercion (*vis absoluta*), which excludes the criminal unlawfulness of the victim’s own conduct. In such a case, the true subject of the crime (through the institution of indirect perpetration) should be recognized as the neurohacker. However, in practice, proving the fact of such interference without sophisticated neurophysiological expertise and digital forensic analysis of neurodevices will be nearly impossible.

Given the transnational nature of cyberspace, the problem of neurohacking also reaches the level of international criminal law. The existing Budapest Convention on Cybercrime¹² does not take into account the specific nature of “bio-digital” encroachments. The use of neurotechnologies for mass control over the consciousness of a population, which is entirely conceivable under authoritarian regimes, may be regarded as a new form of crimes against humanity¹³. At the national level, legislation aimed at prevention requires the supplementation of the Special Part of the Criminal Code¹⁴ with a new section, or at least new articles (*sui generis*), that would criminalize “Unauthorized interference with the mental sphere of an individual through the use of neurotechnologies,” including the construction of qualifying circumstances such as the commission of the act against a minor, for profit motives, or by an organized group.

¹¹ Гороховська О. В. Межі криміналізації втручання у психічну сферу особи засобами віртуальної реальності. *Часопис Київського університету права*. 2023. № 2. С. 211–218.

¹² Конвенція про кіберзлочинність. *Верховна Рада України*. URI: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 12.03.2026).

¹³ Комаров В. В. Кібербезпека та когнітивна недоторканність у європейському кримінальному праві. *Правова держава*. 2021. № 42. С. 98–106.

¹⁴ Кримінальний кодекс України. *Верховна Рада України*. URI: <https://zakon.rada.gov.ua/laws/show/2341-14>

Only such a comprehensive approach, combining a philosophical and legal rethinking of cognitive autonomy with a clear doctrinal construction of new elements of criminal offenses, is capable of ensuring adequate protection of the individual in the context of the inevitable neurotechnological revolution.

2. The Doctrine of "Digital Dignity" (Protection Against Algorithmic Manipulation and Deepfakes)

2.1. Evolution of the concept of dignity: "digital dignity" as an independent legal value in the era of Web 3.0 and artificial intelligence

The development of the information society, the transition to the era of Web 3.0, and the total integration of artificial intelligence (AI) systems into all spheres of human activity have led to an irreversible transformation of the ontological status of the individual. Historically, the category of human dignity was formed as a fundamental philosophical and legal imperative that prohibits treating a person merely as a means to achieve an end. In classical criminal law, dignity served as a basic criterion for the protection of life, health, liberty, and honor of the individual in the material world. However, within the contemporary technological landscape, the physical body has ceased to be the sole repository of identity. A significant portion of an individual's social, economic, and political existence has shifted into virtual space, where the person exists in the form of a complex aggregate of data, which creates an imperative need to establish a new legal category – digital human rights^{15 16}.

The human being emerges as a living informational organism. At present, however, the essence of the person is inseparably and organically connected with their digital footprint¹⁷. Under this approach, personal data, biometric profiles, digital avatars, and behavioral patterns are regarded not merely as alienable property or external information, but as a direct continuation of the personality – its "digital twin." Accordingly, any unauthorized interference, distortion, or exploitation of this digital twin causes harm not only to the right to privacy but also affects the very foundation of human self-respect and autonomy, which requires the doctrinal recognition of digital dignity as an independent legal value.

Within the context of criminal law doctrine, the recognition of digital dignity as either a generic or a direct object of legal protection constitutes a revolutionary yet necessary step. Traditional postmodern criminal-law scholarship often proves powerless in addressing crimes where no tangible material or physical damage is present, yet enormous harm is inflicted upon a person's reputation and social status in the virtual environment. Digital dignity as a direct object of crime signifies a state guaranteed by the state in which an individual's digital identity is protected from

¹⁵ Харитонов С. О., Харитонova О. І. Цифрові права людини: концептуальні засади. *Юридичний науковий електронний журнал*. 2022. № 4. С. 112–118.

¹⁶ Барабаш Ю. Г. Цифрова гідність: конституційно-правовий та кримінальний аспекти. *Право України*. 2023. № 2. С. 89–97.

¹⁷ Шуба І. В., Солошук М. М., Сидоренко О. В. Цифровий слід особистості. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я*. 2022. С. 871. URL: <https://repository.kpi.kharkov.ua/server/api/core/bitstreams/450cc2f3-2cb7-4900-a646-1789c1428e0b/content> (дата звернення: 12.03.2026).

depersonalization, algorithmic discrimination, the creation of false digital representations, and the commercial exploitation of behavioral characteristics without informed consent.

Comparative legal analysis demonstrates a gradual shift in emphasis within the European legal tradition. For example, the German constitutional doctrine, based on the absolute protection of human dignity (Article 1 of the Basic Law of the Federal Republic of Germany – Menschenwürde¹⁸), is currently being actively adapted by courts to the digital environment, recognizing the right to informational self-determination as part of the general right of personality. At the same time, in the criminal-law sphere a fragmented approach still prevails: copyright protection applies separately to content, personal data are protected separately, and the secrecy of correspondence is regulated independently. The concept of digital dignity proposes an integrative approach whereby criminal law should comprehensively safeguard the individual's right not to be reduced to a set of algorithmically calculated parameters (profiling) and not to have their digital image manipulated. The absence of such a comprehensive object complicates the qualification of modern cybercrimes, transforming them into latent or unpunished acts.

2.2. Criminal-law qualification of the creation and dissemination of deepfakes: violation of identity and reputational harm

Deepfake technology¹⁹, based on the use of generative adversarial networks (GANs) for the synthesis of realistic images, videos, and audio materials, has emerged as one of the most dangerous instruments of encroachment upon digital dignity.

The ability of machine-learning algorithms to imitate with high precision the appearance, facial expressions, and voice of a specific individual erases the boundary between authentic fact and synthesized falsification. From the perspective of criminal law, the creation and dissemination of deepfakes with malicious intent constitute a complex multi-object offense that simultaneously threatens a person's honor, dignity, reputation, mental health, property rights, and, in cases of political application, national security and the foundations of democratic governance.

Existing national and European criminal-law systems encounter serious difficulties in qualifying actions related to deepfakes. Attempts to apply traditional norms concerning defamation, fraud, extortion, or violations of privacy often prove legally inadequate. A classic example is the creation of pornographic deepfakes (so-called non-consensual intimate imagery – NCII). In such cases, the dissemination does not formally involve the disclosure of private-life secrets, since the depicted intimate scenes never occurred in objective reality²⁰. Consequently, the subject

¹⁸ Основний закон ФРН. 1949. Зі змінами та доповненнями від 19.12.2022. URL: https://www.bundestag.de/resource/blob/1033364/grundgesetz_uk.pdf (дата звернення: 12.03.2026).

¹⁹ Bhandari R., Bhandari S. Artificial intelligence: understanding deepfakes. 2025. URL: <https://www.tandfonline.com/doi/abs/10.1080/07366981.2025.2484863> (date of access: 12.03.2026). DOI: <https://doi.org/10.1080/07366981.2025.2484863>

²⁰ Viola M., Voto C. Designed to abuse? Deepfakes and the non-consensual diffusion of intimate images. *Synthese*. 2023. URL: <https://link.springer.com/content/pdf/10.1007/s11229-022-04012-2.pdf> (date of access: 12.03.2026). DOI: <https://doi.org/10.1007/s11229-022-04012-2>

matter of the crime in its traditional understanding is absent. Nevertheless, the psychological trauma, stigmatization, and reputational harm inflicted upon the victim are enormous and often exceed the consequences of disseminating authentic intimate materials. This demonstrates the existence of a critical gap in criminal legislation²¹, which requires the construction of a specific criminal offense whose object would be precisely digital identity and dignity.

International experience offers several approaches to resolving this issue. In the United States, the criminalization of deepfakes largely occurs at the level of individual state legislation (for example, California, Virginia, and Texas), where specific laws criminalize the dissemination of synthetic intimate materials without the individual's consent, as well as the use of deepfakes to influence election outcomes during a defined period prior to voting day. The United Kingdom adopted the Online Safety Act in 2023, which explicitly criminalized the distribution of deepfake pornography without consent, establishing strict sanctions regardless of whether the offender intended to cause harm, focusing instead on the mere fact of violating consent regarding the use of a person's image.

The construction of the objective element (*actus reus*) of such an offense in national legislation requires a precise distinction between lawful uses of generative AI (in cinematography, satire, or artistic expression, where freedom of expression applies) and criminally punishable conduct. The decisive criterion should be the combination of two elements: the absence of the individual's informed consent to the use of their biometric data (face, voice) and the existence of socially dangerous consequences or the intent to cause them. The very fact of unauthorized exploitation of biometric parameters in order to create the illusion of actions or statements is regarded by European scholars as an act of digital identity theft²².

The subjective element (*mens rea*) of crimes related to deepfakes is characterized exclusively by an intentional form of guilt, most often direct intent. The offender is aware that they are generating falsified content and desires the occurrence of specific consequences: misleading the public, destroying a person's business reputation, or obtaining financial gain. The latter is particularly evident in cases of so-called CEO fraud, where a deepfake of a company executive's voice is used to authorize the transfer of corporate funds. In such situations, the deepfake functions as a high-technology method of committing fraud (through deception), which requires the introduction of an appropriate qualifying element within offenses against property.

²¹ Юртаєва К. В. Кримінологічний аналіз використання технології deepfake: коли фейк стає злочином. *Вісник кримінологічної асоціації України*. 2021. № 1(24). С. 31–42. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/f94ec02c-eb36-4adc-8cf5-c121c5580020/content> (дата звернення: 12.03.2026).

²² Burrell D. N. The Cyberpsychology and Criminal Psychology of Cyber Identity Theft and Criminal Reach in the Digital Era. *«Rais» Journal for social sciences*. 2025. Vol. 9, № 2. P. 343–353. URL: <https://journal.raiss.education/index.php/raiss/article/view/302/249> (date of access : 12.03.2026).

2.3. Algorithmic manipulation of consciousness: establishing the boundary between aggressive marketing and socially dangerous criminal encroachment

The everyday functioning of a modern individual within the digital environment is determined by continuous interaction with recommendation algorithms, search engines, and social networks. Within the global economic model, attention and emotional reactions have become raw material for data extraction, predictive analysis, and subsequent monetization. In this context, machine-learning algorithms have long moved beyond the passive representation of information; they are now used for the active formation of needs, modification of beliefs, and direct influence over users' decisions. Criminal law thus faces an exceptionally complex doctrinal task: to establish a clear boundary between lawful, albeit aggressive, digital marketing and algorithmic manipulation of consciousness that reaches the level of social danger characteristic of a criminal offense.

To resolve this issue, it is necessary to turn to a deeper doctrinal distinction between the concepts of persuasion, coercion, and manipulation. As philosophers of law Daniel Susser, Beate Roessler, and Helen Nissenbaum rightly observe, persuasion appeals to the rational thinking of the subject, providing transparent arguments that allow for conscious choice. Manipulation, by contrast, possesses a latent character; it deliberately exploits cognitive biases, emotional vulnerabilities, and subconscious triggers, thereby circumventing an individual's capacity for critical reflection on reality²³. From the perspective of criminal law, algorithmic manipulation constitutes a direct encroachment upon the autonomy of will: the subject makes a legally significant decision (regarding property, participation in mass disturbances, or the incitement of hostility), falsely believing it to be an expression of their own free will, whereas in reality it was rigidly determined by external computational intervention through the so-called "choice architecture" or "dark patterns." Until recently, scholarly attention focused primarily on "traditional" dark patterns that rely on weaknesses in human cognition. Various classifications of dark patterns have been developed in order to facilitate their identification and regulation. However, increasing attention is now being devoted to the role of artificial intelligence in such patterns and to the ways in which this may affect the end consumer – the human being. In particular, the Polish researcher Agnieszka Kitkowska carefully analyzes hypothetical scenarios of AI-driven dark patterns as well as the negative consequences they may produce²⁴.

Modern micro-targeting technologies employing methods of deep psychometric profiling (similar to the mechanisms revealed during the Cambridge Analytica scandal) enable the creation of extremely personalized informational stimuli. When an algorithm, after analyzing the digital traces of a user, detects a tendency toward depression or impulsive behavior and deliberately bombards that user with content designed to intensify those states in order to maximize engagement or promote the sale of goods, this constitutes algorithmic violence. The social danger of such

²³ Susser D., Roessler B., Nissenbaum H. Technology, autonomy, and manipulation. *Internet Policy Review*. 2020. Vol. 9, № 2. URL: <https://policyreview.info/articles/analysis/technology-autonomy-and-manipulation> (дата звернення: 12.03.2026).

²⁴ Kitkowska A. Chapter 19: The AI-empowered dark patterns. 2025. DOI: <https://doi.org/10.4337/9781035300198.00028>

conduct is unprecedented because of its scale, automation, and absolute concealment, which makes it a far more powerful instrument of social engineering than any traditional forms of psychological or physical influence.

A fundamental guideline for determining the boundaries of criminalization in this sphere is provided by the recently adopted and previously mentioned Regulation (EU) of the European Parliament and of the Council on artificial intelligence (AI Act). The provisions of this landmark document imperatively prohibit the placing on the market, deployment, or use of AI systems that apply subliminal techniques beyond a person's consciousness in order to materially distort their behavior, where this causes or is likely to cause physical or psychological harm to an individual. The exploitation of vulnerabilities of specific groups (due to age, physical condition, or mental disability) is likewise prohibited. Article 5 of the Regulation effectively recognizes subconscious algorithmic manipulation as conduct that grossly violates fundamental human rights. The transposition of this regulatory provision into the sphere of national criminal law implies that the intentional use of such algorithms for financial gain should be qualified as a particularly serious form of high-technology fraud, and where used with the aim of driving a person to suicide or causing harm to mental health, as the corresponding offense against life and health, with AI functioning as a specific instrument of the crime.

However, proving the fact of criminally punishable manipulation within criminal proceedings presents a significant challenge for law-enforcement authorities. The principal difficulty lies in establishing a legally significant causal link between the architecture of a recommendation algorithm and the specific harm suffered by the victim. Moreover, the issue of identifying the subject of the crime becomes particularly acute: who should bear criminal liability? Is it the developer corporation (which raises the issue of criminal liability of legal entities), the specific data scientists and programmers who created the system, or the company's top management that consciously approved a business model built upon the algorithmic exploitation of human vulnerabilities?

The resolution of these doctrinal and practical issues requires the development of new institutions of digital forensics and independent algorithmic auditing. Such mechanisms would make it possible to establish a clear demarcation line between permissible marketing strategies, which operate within the framework of transparency and the informed consent of the user, and covert information-psychological operations that undermine the digital and cognitive integrity of the individual. Effective criminal-law protection against algorithmic manipulation is an absolute prerequisite for preserving human legal subjectivity in the era of strong artificial intelligence. Without guaranteeing the right to freely form one's own will, free from the invisible dictates of corporate algorithms, the very concept of individual criminal responsibility and guilt loses its ontological and legal meaning.

3. The Right to Non-Algorithmic Existence (Legal and Theoretical Justification of Infringements on the Autonomy of Choice)

3.1. The essence and ontological content of the right to non-algorithmic existence

The fundamental shift in the paradigm of social development, caused by the ubiquitous integration of artificial intelligence systems and machine-learning algorithms into the architecture of social institutions, requires the science of criminal law to reconsider the very ontological foundations of human existence. Society is currently transitioning from a stage in which algorithms performed exclusively auxiliary or advisory functions to a state of algorithmic governance, where mathematical models make legally significant decisions regarding credit allocation, employment opportunities, access to medical services, and even an individual's propensity to commit crimes through predictive policing. In this context, there arises an urgent need to conceptualize a new generation of human rights, among which the "right to non-algorithmic existence" occupies a central place as a guarantee of preserving human essence in conditions of total digital quantification.

The right to non-algorithmic existence should not be equated with neo-Luddism or a categorical rejection of technological progress. Its ontological content lies in preserving for the human being the prerogative of unpredictability, irrationality, the right to make mistakes, and the capacity for moral development beyond rigidly predetermined mathematical parameters and predictive models. The doctrinal essence of this right is based on the recognition that a human being is far more than merely a set of biometric data and digital traces that can be calculated, predicted, and monetized. Encroachment upon this sphere through the forced algorithmization of life processes constitutes a direct threat to human dignity, as it reduces a unique personality to the level of a statistical deviation or a standardized cluster within a database.

Within the framework of criminal-law doctrine, the right to non-algorithmic existence is closely linked to the category of free will, which serves as a cornerstone of the institution of criminal responsibility and guilt. If the behavior of the subject, their choices, preferences, and intentions are continuously and imperceptibly corrected, shaped, or blocked by external algorithms – from curated news feeds to algorithmic routing of movement – serious doubts arise regarding the existence of a genuine volitional element in their actions. Postmodern criminal law thus encounters a paradox: when an algorithm determines the horizon of possibilities available to a subject by restricting access to alternative information, can we truly assert that a subsequent socially dangerous act (for example, a hate crime induced by the consumption of radicalized content) is solely the product of the individual's personal guilt? Protecting the right to non-algorithmic existence therefore becomes, in essence, the protection of the very structure of the subjective element of crime (*mens rea*).

The genesis of the legal recognition of this right has already begun within the European legal sphere. Article 22 of the General Data Protection Regulation (GDPR)²⁵ establishes the right of the data subject not to be subject to a decision

²⁵ Загальний регламент про захист даних (GDPR). URL: <https://gdpr-text.com/uk/> (дата звернення: 12.03.2026).

based solely on automated processing, including profiling, which produces legal consequences for them. However, the current administrative and civil-law instruments are no longer sufficient. There is an urgent need to extrapolate this principle to the level of constitutional guarantees and criminal-law prohibitions. The compulsory inclusion of an individual in systems of social scoring or predictive analysis without their conscious consent should be recognized as a socially dangerous act – an encroachment upon their cognitive and digital integrity.

The theoretical and legal justification for criminalizing violations of the autonomy of choice is based on recognizing algorithmic coercion as an independent form of violence. Classical criminal law acknowledges physical or psychological violence as circumstances influencing the qualification of an act or excluding criminal liability. The information society, however, generates a new phenomenon – algorithmic violence: an invisible structural pressure exerted by computational systems that deprives the individual of subjectivity and imposes a predetermined model of behavior. This reality requires the development of an entirely new doctrinal institution within criminal law. Accordingly, compulsory profiling and the deprivation of an individual's right to an alternative, human review of their status or case should receive a strict criminal-law evaluation as conduct that infringes upon the fundamental rights and freedoms of the person.

3.2. Algorithmic determinism and “filter bubbles” as a threat to free will and personal autonomy (criminal law dimension)

The concept of algorithmic determinism describes the state of a digital environment in which the choices presented to a user are predetermined and strictly constrained by personalized recommendation systems. Platform algorithms, aiming to maximize user engagement time and corporate profit, continuously analyze an individual's digital footprint and create a so-called “filter bubble” around them²⁶. This phenomenon leads to a state of epistemic isolation: the individual consumes exclusively information that confirms their preexisting biases and is deprived of access to alternative perspectives, creating the illusion of complete freedom of choice in the absence of actual autonomy. From the perspective of criminal policy, the artificial narrowing of an individual's cognitive horizon constitutes a latent but highly potent threat to societal security.

The criminal law dimension of filter bubbles and echo chambers is most prominently manifested in processes of mass radicalization. Contemporary research convincingly demonstrates that social media algorithms are prone to promote emotionally charged, extremist, and polarizing content, as such material elicits the strongest neurobiological responses in users. When an individual predisposed to certain biases enters such an algorithmic funnel, the system deliberately and systematically drives them into a state of affective arousal or fanaticism, which frequently culminates in acts of terrorism, mass unrest, or hate crimes. In this paradigm, the algorithm effectively functions as a “digital instigator,” prompting a re-evaluation of the concept of complicity in criminal law.

²⁶ Drewes H. The Fitts' Law Filter Bubble. 2023. P. 1–5. DOI: <https://doi.org/10.1145/3544549.35827>

Analyzing the objective aspect (*actus reus*) of such algorithmic facilitation of criminality, criminalists face an unprecedented challenge: can the architecture of program code, which automatically generates recommendations without the direct involvement of a human moderator in each individual case, be considered an instrument or means of committing a crime? If the developer corporation is aware that its algorithm contributes to radicalization but deliberately does not modify its code to preserve profits (employing so-called “dark patterns”), its actions (or criminal omission) cross the boundary of ethical violation and acquire the characteristics of a punishable offense. This raises the question of establishing corporate criminal liability for designing AI systems that create unacceptable risks to societal stability and individual autonomy.

An even more complex issue is the assessment of the impact of algorithmic determinism on the subjective aspect of a crime committed by the user themselves. Prolonged exposure to a toxic informational environment modeled by AI can induce profound changes in the subject’s psyche, effectively reprogramming their moral imperatives. In legal-theoretical doctrine, a contentious question arises: can prolonged algorithmic “brainwashing” be regarded as a form of irresistible mental coercion, which, if it does not fully exclude criminal liability, at least constitutes a mitigating circumstance (diminished responsibility)? Distinguishing between a state of medical insanity and a state of deep cognitive manipulation will require the development of novel forensic psychiatric methodologies for evaluating “algorithmic dependency” and loss of autonomy.

Beyond radicalization, encroachments on autonomy of choice manifest through algorithmic nudging toward disadvantageous financial or legal actions. The use of microtargeting to identify an individual’s psychological vulnerabilities (for example, a predisposition to gambling addiction) followed by a bombardment of personalized online casino advertisements constitutes nothing less than high-tech extortion or fraud. In this context, the boundary between aggressive platform architecture and criminally punishable conduct lies in the exploitation of the victim’s vulnerable state through algorithmic means. Accordingly, criminal law must recognize that cyberspace, constructed on manipulative models, is an environment in which free will is systematically and massively suppressed, demanding an adequate and stringent response from the state.

3.3. Prospects for implementing protection against algorithmic coercion in national and international criminal legislation

The current system of international and national criminal law, built primarily on responding to the consequences of traditional (physical or property-based) offenses, proves conceptually incapable of effectively countering the threats posed by algorithmic coercion and neuromanipulation. The existing Budapest Convention on Cybercrime²⁷ focuses on protecting the confidentiality, integrity, and availability of computer systems (hardware and software), leaving the protection of human consciousness as the ultimate recipient of digital influence outside the scope of legal

²⁷ Конвенція про кіберзлочинність. 2021. URL: <https://ips.ligazakon.net/document/MU01209> (дата звернення: 12.03.2026).

regulation. Accordingly, there is an urgent need to shift the doctrinal paradigm from reactive (consequence-based) regulation to a preventive approach, in which criminal law establishes clear boundaries (red lines) for developers of artificial intelligence systems.

A fundamental step toward creating such an international legal framework was the adoption of the European Parliament and Council Regulation (EU) 2024/1689 on artificial intelligence (AI Act). For the first time in history, this document applied a risk-oriented approach to technology classification, categorically prohibiting AI systems that employ subconscious manipulation methods acting outside of human awareness, as well as social scoring systems that result in unjustified or disproportionate harm. However, the AI Act currently functions as an administrative-regulatory instrument. To ensure effective protection of cognitive integrity, its provisions must be transposed into the national criminal codes of member states and candidate countries, requiring comprehensive legislative reform.

Doctrinal perspectives on implementation foresee the addition to the Special Part of the Criminal Code of Ukraine of a new section or a separate group of norms criminalizing “Encroachment on digital autonomy and cognitive inviolability of the individual.” The main elements of such an offense could include liability for: “The intentional development, deployment, or use of artificial intelligence systems or algorithms with the purpose of covert manipulative influence on the consciousness of an individual or group, resulting in substantial distortion of their behavior, harm to health, property damage, or endangerment of public security.” Aggravating circumstances could include actions committed against minors, the use of data concerning psychological vulnerabilities (neurodata), or actions undertaken by an organized group in the interest of a foreign state (which may constitute information terrorism).

The specific construction of these offenses requires the introduction of the concept of “algorithmic complicity.” In cases where an algorithm independently evolves and begins causing harm (operating beyond the control of its creator), classical theories of intent face significant challenges. Legal scholarship proposes resolving this issue through the concept of “indirect causation” and design negligence: if a developer deliberately ignored safety protocols and ethical standards during the training of a neural network (failing to eliminate algorithmic bias), they bear full criminal responsibility for the socially dangerous consequences generated autonomously by the system. This necessitates the creation of specialized units in law enforcement for “algorithmic forensics,” capable of reverse engineering AI code to demonstrate intent or corporate criminal negligence.

Moreover, considering the transnational nature of cyberspace and the extraterritorial operations of global technology giants, effective protection of the right to non-algorithmic existence is impossible without the adoption of a new specialized international convention – the Convention on the Protection of Neuro-Rights and Digital Inviolability. A reference point for this could be the Council of Europe’s Declaration on the Protection of Neuro-Rights in the Digital Age. Such a convention should not only unify the dispositions of crimes related to algorithmic manipulations for all signatory states but also establish effective mechanisms of

international legal assistance in requesting source code and training datasets from transnational corporations during criminal investigations.

In conclusion, it should be emphasized that the criminal-law protection of cognitive and digital integrity is not an attempt to hinder technological innovation. On the contrary, it is the only path to ensuring sustainable and human-centric technological development. By establishing criminal liability for encroachments on autonomy of choice and the use of manipulative algorithms, the state fulfills its most crucial function in the 21st century: protecting the ontological essence of the human being from deconstruction and absorption by digital environments, preserving the primacy of reason in making free decisions.

CONCLUSIONS

The comprehensive theoretical and legal study of the protection of cognitive and digital integrity of the individual in the context of the development of neurotechnologies and artificial intelligence systems allows for the formulation of the following key scientific conclusions.

The rapid evolution of convergent technologies, particularly neuromodulation and brain-computer interfaces, has caused an unprecedented shift in the paradigm of criminal law. The historically established presumption of inviolability of only the physical body proves insufficient in an era when the human mind becomes a vulnerable informational node. The necessity for immediate doctrinal recognition and enshrinement, at the level of objects of criminal-law protection, of a new category-neuro-rights (including cognitive freedom, mental inviolability, and psychological continuity) – has been demonstrated. It has been established that classical cybercrime is evolving into so-called “neurohacking,” the societal danger of which lies not merely in the theft of personal data but in the direct, unauthorized interference in the formation of thoughts, emotions, and neurobiological responses, fundamentally undermining the subjectivity of the individual and the core freedom of their will.

The transition of social and economic existence into virtual environments (Web 3.0) justifies the urgent need to introduce the concept of “digital dignity” as an independent and comprehensive legal good into the doctrine of the Special Part of criminal law. The modern individual exists not only in the physical dimension but also in the form of a “digital double.” Accordingly, traditional criminal offenses (fraud, defamation, invasion of privacy) are doctrinally insufficient to counter such new threats as deepfakes. The use of generative AI to create synthetic materials without the informed consent of the individual constitutes an independent act of “digital identity theft,” requiring the construction of special criminal-law norms (*sui generis*) to guarantee protection of reputation and inviolability of the subject’s virtual image.

The total algorithmization and automation of social processes transforms algorithmic coercion into a new, latent form of violence. The malicious use of recommendation systems, the formation of filter bubbles, and the application of subconscious targeted influence methods for mass manipulation of choice represent a direct encroachment on the right of the individual to a non-algorithmic existence. Drawing on advanced European experience (particularly the provisions of the EU AI Act), the need for a clear criminal-law distinction between aggressive marketing and socially dangerous informational influence has been substantiated. The use of

algorithms to exploit cognitive vulnerabilities with the aim of inducing suicide, appropriating property, or radicalizing individuals (inducing hate-based crimes) should be qualified with new aggravating circumstances, where AI acts as a specific high-tech instrument of crime.

The paradigm of national and international criminal law requires an urgent shift from a reactive model (responding to physical or property consequences) to a preventive model of legal regulation of algorithmic systems. Effective protection of cognitive and digital integrity will require fundamental modernization of criminal justice:

- the introduction of the institution of algorithmic forensics for conducting independent code audits and establishing causal links between AI architecture and harm caused;

- the revision of doctrinal concepts of intent and complicity through the lens of “algorithmic facilitation,” raising questions of corporate criminal liability (of developer corporations) for negligent training of neural networks;

- the adoption of a specialized international Convention on the Protection of Neuro-Rights and Digital Inviolability, which would unify approaches to extraterritorial investigation of crimes against human consciousness.

In conclusion, it should be emphasized that the criminal-law protection of cognitive and digital integrity is not an attempt to halt technological progress. On the contrary, it is the only legal instrument for ensuring the sustainable, human-centric development of civilization. By establishing strict criminal liability for encroachments on autonomy of choice, the state fulfills its highest mission in the 21st century-protecting the ontological essence of the human being from deconstruction by digital environments while preserving for the human mind the exclusive monopoly over freedom of will and decision-making.

SUMMARY

The article “Protection of Cognitive and Digital Integrity of the Individual” presents a comprehensive theoretical and legal study of the mechanisms for ensuring human internal and digital autonomy in the context of the expansion of neurotechnologies and artificial intelligence systems. The author justifies the need for criminal law protection of neuro-rights, examining the theoretical foundations of criminalizing unauthorized interference in the mental sphere as a critical condition for preserving cognitive freedom. Particular attention is paid to the development of the doctrine of “digital dignity,” which serves as a tool to counter algorithmic manipulation and the spread of deepfake technologies that threaten the authenticity of one’s personal image. For the first time, this study systematically presents a theoretical and legal justification for the right to non-algorithmic existence as a fundamental challenge to the autonomy of human choice. This right is viewed as a response to contemporary challenges to the autonomy of human choice arising from the pervasive influence of recommender systems and predictive analytics. It is demonstrated that preserving genuine subjectivity in the digital age requires the normative enshrinement of an individual’s right to make legally significant and vitally important decisions outside the bounds of algorithmic pressure. The conclusions formulated by the author are aimed at a conceptual rethinking of the

institution of human rights through the lens of an anthropocentric approach, which will effectively protect human consciousness from technological determinism and ensure a balance between innovative development and legal security.

References

1. Регламент Європейського Парламенту та Ради (ЄС) 2024/1689 щодо встановлення гармонізованих правил щодо штучного інтелекту (AI Act). *Офіційний вісник Європейського Союзу*, 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 12.03.2026).
2. Радутний О. Е. Кримінально-правовий вимір штучного інтелекту та нейротехнологій. *Право та інновації*. 2021. № 1. С. 56–63.
3. Гуторова Н. О. Ментальна недоторканність як об'єкт кримінально-правової охорони у цифрову епоху. *Вісник Асоціації кримінального права*. 2022. № 1. С. 120–129.
4. Туляков В. О. Кримінальне право постмодерну та виклики алгоритмізації. *Слово Національної школи суддів*. 2022. № 3. С. 45–52.
5. Барабаш Ю. Г. Цифрова гідність: конституційно-правовий та кримінальний аспекти. *Право України*. 2023. № 2. С. 89–97.
6. Наїф аль Родхан Нейротехнології та нейроправа. URL: <https://zbruc.eu/node/105492> (дата звернення: 12.03.2026).
7. Нестеренко О. В., Яцук П. П. ШІ (не) проти ШІ. *Екологічна безпека та природокористування*. 2025. Вип. 4 (56). С. 134–153. URI: <http://e.ieu.edu.ua/handle/123456789/1414> (дата звернення: 12.03.2026).
8. Шевцов А. Г. Критичний аналіз поняття «свідомості» в сучасній методології штучного інтелекту. *Технології розвитку інтелекту*. 2025. Т. 9, № 1 (37). С. 1–22. DOI: <https://doi.org/10.31108/3.2025.9.7>
9. Орловський М. С., Іващенко С. М. Мультимодальні реабілітаційні стратегії у подоланні фантомного болю: огляд інноваційних практик та перспективи розвитку. *Неврологія*. 2025. С. 89–97. DOI: <https://doi.org/10.31640/LS-2026-1-10>
10. Ienca M., Scheibner J. Chapter Eight – What is neurohacking? Defining the conceptual, ethical and legal boundaries. 2020. Vol. 3. DOI: <https://doi.org/10.1016/bs.dnb.2020.03.008>
11. Гороховська О. В. Межі криміналізації втручання у психічну сферу особи засобами віртуальної реальності. *Часопис Київського університету права*. 2023. № 2. С. 211–218.
12. Конвенція про кіберзлочинність. *Верховна Рада України*. URI: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 12.03.2026).
13. Комаров В. В. Кібербезпека та когнітивна недоторканність у європейському кримінальному праві. *Правова держава*. 2021. № 42. С. 98–106.
14. Кримінальний кодекс України. *Верховна Рада України*. URI: <https://zakon.rada.gov.ua/laws/show/2341-14>
15. Харитонов Є. О., Харитонova О. І. Цифрові права людини: концептуальні засади. *Юридичний науковий електронний журнал*. 2022. № 4. С. 112–118.
16. Барабаш Ю. Г. Цифрова гідність: конституційно-правовий та кримінальний аспекти. *Право України*. 2023. № 2. С. 89–97.

17. Шуба І. В., Солощук М. М., Сидоренко О. В. Цифровий слід особистості. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я*. 2022. С. 871. URL: <https://repository.kpi.kharkov.ua/server/api/core/bitstreams/450cc2f3-2cb7-4900-a646-1789c1428e0b/content> (дата звернення: 12.03.2026).
18. Основний закон ФРН. 1949. Зі змінами та доповненнями від 19.12.2022. URL: https://www.bundestag.de/resource/blob/1033364/grundgesetz_uk.pdf (дата звернення: 12.03.2026).
19. Bhandari R., Bhandari S. Artificial intelligence: understanding deepfakes. 2025. URL: <https://www.tandfonline.com/doi/abs/10.1080/07366981.2025.2484863> (date of access: 12.03.2026). DOI: <https://doi.org/10.1080/07366981.2025.2484863>
20. Viola M., Voto C. Designed to abuse? Deepfakes and the non-consensual diffusion of intimate images. *Synthese*. 2023. URL: <https://link.springer.com/content/pdf/10.1007/s11229-022-04012-2.pdf> (date of access: 12.03.2026). DOI: <https://doi.org/10.1007/s11229-022-04012-2>
21. Юрасва К. В. Кримінологічний аналіз використання технології deepfake: коли фейк стає злочином. *Вісник кримінологічної асоціації України*. 2021. № 1(24). С. 31–42. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/f94ec02c-eb36-4adc-8cf5-c121c5580020/content> (дата звернення: 12.03.2026).
22. Burrell D. N. The Cyberpsychology and Criminal Psychology of Cyber Identity Theft and Criminal Reach in the Digital Era. *«Rais» Journal for social sciences*. 2025. Vol. 9, № 2. P. 343–353. URL: <https://journal.raiss.education/index.php/raiss/article/view/302/249> (date of access : 12.03.2026).
23. Susser D., Roessler B., Nissenbaum H. Technology, autonomy, and manipulation. *Internet Policy Review*. 2020. Vol. 9, № 2. URL: <https://policyreview.info/articles/analysis/technology-autonomy-and-manipulation> (дата звернення: 12.03.2026).
24. Kitkowska A. Chapter 19: The AI-empowered dark patterns. 2025. DOI: <https://doi.org/10.4337/9781035300198.00028>
25. Загальний регламент про захист даних (GDPR). URL: <https://gdpr-text.com/uk/> (дата звернення: 12.03.2026).
26. Drewes H. The Fitts' Law Filter Bubble. 2023. P. 1–5. DOI: <https://doi.org/10.1145/3544549.35827>
27. Конвенція про кіберзлочинність. 2021. URL: <https://ips.ligazakon.net/document/MU01209> (дата звернення: 12.03.2026).

Information about the author:

Kravchuk Svitlana Mykolaivna,

Senior Lecturer at the Department of Theory of Law and Constitutionalism
Educational and Scientific Institute of Law, Psychology,
and Innovative Education,

Lviv Polytechnic National University,
12, Stepan Bandera str., 79013, Lviv, Ukraine
Juror of the Shevchenkivskyi District Court of Lviv
<https://orcid.org/0000-0002-3485-1343>