Legal Issues in the Digital Age. 2025. Vol. 6, no. 2.
Вопросы права в цифровую эпоху. 2025. Том 6. № 2.

Research article
JEL: K 00
UDK: 34.096
DOI:10.17323/2713-2749.2025.2.134.160

Brain-Computer Interface 5.0: Potential Threats, Computational Law and Protection of Digital Rights

Said S. Gulyamov

Tashkent State University of Law, 7 Iftihor, 8 Yunusabad,Tashkent, Uzbekistan 100057,

said.gulyamov1976@g.mail.com, ORCID: https://orcid.org/0000-0002-2299-2122,

Abstract

The development of neurotechnologies is now at a critical point where direct readout and modulation of brain activity has passed from test studies to business applications, only to urgently require adequate legal and technological guarantees. The relevance of this study is prompted by the rapid development of the fifth generation brain-computer interface (BCI 5.0), a technology that provides unprecedented potential of direct access to neural processes while at the same time creating principally new threats to digital rights of individuals. The existing legal mechanisms have turned out to be inadequate for regulating altogether new risks of manipulating consciousness, unauthorized access to neural data and compromised cognitive autonomy. The study is focused on legal and technological mechanisms for protection of digital rights in the context of introducing the fifth generation neural interface technologies including analysis of regulatory gaps, technical vulnerabilities and possible security guarantees. Methodologically, the study is based on the multidisciplinary approach bringing together neuroscience, law and information technology, and on the comparative analysis of regulatory framework and inductive inference of specific regulatory mechanisms. The main hypothesis is: legacy regulatory mechanisms for data protection in biometric and telecommunication technologies are structurally inadequate for BCI 5.0 while digital rights could be protected only by a hybrid system combining special provisions with technological guarantees via mechanisms of computational law. The author puts forward a minimum set of viable security and confidentiality standards, comprehensive cryptography and blockchain-based applications, as well as detailed legislative advice for ethical and safe neurotechnological development with secure guarantees of fundamental human rights in the digital age. Findings of the study are of considerable practical value for legislators, those involved in the development of neurotechnologies, regulatory bodies and advocacy organizations by proposing specific evidence-based tools and mechanisms to strike an effective balance between the innovative development and the imperatives of protecting human dignity, mental autonomy and cognitive freedom.

Keywords

digital rights; computational law; neural privacy; cognitive freedom; neuron technologies; legal regulation; data protection; ethical governance.

For citation: Gulyamov S.S. (2025) Brain-Computer Interface: Potential Threats, Computational Law and Protection of Digital Rights. *Legal Issues in the Digital Age,* vol. 6, no. 2, pp. 134–160. DOI:10.17323/ 2713-2749.2025.2.134.160

Background

The emergence of brain-computer interface technologies (BCI) opens up an enormous potential not only for improved communication between individuals and computers but also for new opportunities in the event of disability.

However, these rapidly advancing technologies are fraught with altogether new regulatory challenges for digital rights of individuals. This article provides an overview of BCI 5.0 innovations, identifies the main threats to rights, discusses the current regulatory principles worldwide, shows the implications of inefficient legal guarantees and proposes viable technical and policy standards for confidential, safe and responsible introduction of BCI 5.0.

BCI technologies will directly link the brain with external devices bypassing traditional neuromuscular outputs. While BCI 1.0 and 2.0 were only for auxiliary applications for locomotor and communication disabilities, BCI 3.0 offers a basic device control potential by analyzing EEG, and BCI 4.0 is capable of hands-free texting, web browsing and gaming at up to 60 characters per minute. BCI 5.0 will elevate these capabilities to a new height through a high-density wireless EEG for seamless conversation, unrestricted environmental management and access to rich virtual worlds.

For example, Facebook's sensory headband prototype allows people to type by simply thinking while Kernel brain prosthetic aims to reproduce hippocampus memory function, and Neuralink strives to help paralyzed persons to control digital devices using a wireless BCI implant. This is nothing short of a neurotechnological revolution since such an invasive, ubiquitous EEG access will profoundly threaten privacy, security, identity and behavior. Notably, consumer EEG headsets are quite vulnerable to spoofing, signal injection and neural data theft.

It is equally worth noting BCI may be manipulated, only to malignantly alter the user's perception, behavior and memories [Burwell C., 2017: 1–12]. Those patenting such capabilities including Elon Musk's Neuralink are not subject to any mechanism for accountability, compensation of damage or civil supervision of likely harm [Sample M., 2021: 159]. A lack of proper legal protection from these emerging risks creates an instant policy gap to be filled. Thus, the article looks into what has been achieved in terms of protection based on the rights needed to access and contain BCI 5.0 capabilities. It analyzes the threats to individual rights from unauthorized access to neural data, assesses the adequacy of regulatory approaches adopted worldwide for meaningful control of technologies and highlights the need for governance mechanisms to encourage ethical and responsible BCI innovations, broader rights and opportunities available to users in respect of their neural data, and for protection of rights.

BCI 5.0 is emerging in a complex technological landscape shaped by huge neurotechnological changes, fragmented political ecosystems and strong private interests.

The potential disruptive power of BCI 5.0 comes from a number of trends, with the rapid progress of EEG software providing for high-definition wireless sensing [Musk N., 2019].

Portable devices such as headbands have a promise of ongoing ex-vivo brain monitoring [Das S. et al., 2021: 5746]. Advanced machine learning architectures can now decode cognitive states using their EEG signatures whereas new standards of communication such as 5G and WiFi 6 enable real-time data transfer between the brain and a cloud, only to open the door to widely available consumer BCI with unprecedented capabilities. However, with much utility promised, such ubiquitous access creates risk. EEG data carry sensitive markers of identity, psychology and intentionality valuable to advertisers, insurers and public agencies and potentially usable to secretly manipulate emotions, filter information and enable behavioral micro-targeting in an unsolicited way observed in the latest research of Facebook's emotional contamination.

Another issue on the agenda could be neurological discrimination leading, like genetic discrimination, to refusal of opportunities. Brain penetration could also effectively threaten user intentions and memories. Thus, uncontrolled BCI 5.0 systems, apart from their benefits, will critically threaten rights and liberties. These likely implications have been magnified by prevailing policy failures. For the most part, BCI applications are still unregulated and fraught with major legal gaps with regard to data access, confidentiality and security.

For example, direct access to personal thoughts, unlike communication, is not protected while only a few meaningful mechanisms ensure the transparency of BCI audit logs or user control over the joint use of neural data. Options to claim a compensation of damage from neurotechnologies are poorly defined, with a lack of specific guarantees to remove new BCI risks extending the scope of violation even more. In addition, global technology companies fast track BCI commercialization in absence of adequate accountability setups. In this regard, Facebook's aggressive acquisitions assume a combination of persuasive power of social media with direct access to cognitive vulnerabilities.

Technological monopolies would repeatedly get hold of user data for profit and manipulation, only to demonstrate the threats inherent in such access to neural data. Their unparalleled resources and lobbying power can dishabilitate any policy response to protect individual rights. Governance gaps and incentives for anti-social business models make regulation an urgent focal point for assuring public interests.

This study assumes that legacy regulatory mechanisms for data protection in biometric, telecom and computer technologies are structurally inadequate in the face of new capabilities of BCI 5.0 that involve direct access to neural processes. It is assumed that only a hybrid regulatory system combining special provisions with technological guarantees embedded into BCI architecture via computational law mechanisms can effectively protect individual digital rights at the time of the fifth generation neural interface. To test this hypothesis, a profound review of emerging opportunities, constraints and risks of BCI 5.0 is performed to inform the plausible design of comprehensive political and technical guarantees for ethical innovations respectful of user rights promoting socially valuable applications.

It has a sense to discuss the study's purposes and objectives. First, the likely benefits and risks of BCI 5.0 are made clear in the light of modern understanding of neural science and documented technological paths for empirically grounded assessment of problems to be addressed. Second, the article offers an overview of the current legal framework from the perspective of adequacy while also identifying gaps in the meaningful regulation of BCI 5.0 capabilities. It also specifies a key objective: it is necessary to have a minimum set of viable standards and mechanisms for BCI 5.0 adapted to its new technological properties to encourage secure, privacy safe, user-controlled systems. This is followed by a description of extra legislative policies and tools of computational law that will allow individuals to better protect their rights. Finally, one of the purposes is to propose guiding principles and recommendations to various stakeholders on the basis of summarized conclusions.

These purposes entail the following objectives of research: a) an in-depth technical overview of the emerging methods including neural network sensors, focused ultrasound neuromodulation, Neuro Mesh implants and AI architecture to support BCI 5.0 applications; b) classification of likely threats to the above rights including unauthorized data access, user behavior manipulation and compromised security based on documented vulnerabilities and predictive scenarios.

Third, the study includes an analysis of the existing laws and assessment of their outreach to effectively address the issues of BCI potential. Fourth, it provides a description of technological guarantees (such as blockchain, differential privacy, federated learning) which can be harnessed to reduce BCI-related risks and embed policy standards. Fifth, there is a description of specific changes applicable to the effective law and a sample code of conduct or ethics charter for stakeholders in BCI. Lastly, the study purports to identify ways to ensure accountability, dispute resolution and liability assessment within the proposed structure.

The multi-level analysis is intended to design effective policies and technical guidance for ensuring security and ethical focus at the next stage of man-machine integration for developers, regulators and users. Recommendations should strike a balance between encouraging useful applications and designing preventive risk reduction policies by providing a roadmap to responsibly navigate the emerging neurotechnological frontiers.

To achieve the above objectives and test the proposed hypothesis, the study relies on a comprehensive methodology embracing three interrelated approaches.

Multidisciplinary data collection and synthesis. The study brings together a variety of fields of knowledge: technical sources from industry journals (Nature Neuroscience, Neuron, Current Opinion in Neurobiology, Brain-Computer Interfaces) provide the details of new methods of neuron visualization/stimulation. Legal journals (Law Journal of the Higher School of Economics, Journal of Law and Biosciences, Journal of Law) make up the basis for analysis of regulatory implications. Multidisciplinary publications (Science and Society, Philosophy and Technology, Ethics and Information Technology, Innovation and Technology) allow to discuss technical issues in the context of rights, value and governance. As an extra source, patent databases, corporate reports and civil society contributions are used for comprehensive understanding of the BCI landscape.

Comparative analysis and inductive reasoning. The study compares BCI 5.0 extended capabilities with existing mechanisms for protection of data, privacy and security while analyzing gaps between technological capabilities and regulatory framework in various jurisdictions. Based on the identified inconsistencies, special guarantees and supervision mechanisms adapted to the unique properties of BCI technologies are inductively proposed. This approach allows to design political and technical responses to new social and technological challenges.

This methodology provides for empirically grounded, balanced approach to come up with advice that would account for both innovative potential and the need to protect individual rights at the time of the fifth generation neural interfaces.

1. BCI 5.0 Technological Capabilities and Threats

1.1. Detailed Overview of Technological Capabilities and Innovations of BCI 5.0

A number of achievements have enabled a transition from laboratory-based and largely stripped-down iterations to ubiquitous, almost seamless integration of man and computer. SDK, such as Facebook's Brain-2Bot, will use consumer EEG headsets for automatic smart instrument control and environmental navigation free of portable devices. Startups such as Paradromics and Cortical Labs (Table 1) are working to make less heavy EEG sensors for high-density recording through the skin at resolutions comparable to FMRT [Sun Y., 2020: 310–324]. Thanks to the progress of machine learning methods, imagined speech and intended movements are now identified from neural activity together with semantic representations.

Taken together, these trends translate into "hands-free real-time interaction" with digital systems given the sole intent. Whereas an early BCI texting interface would identify EEG correlates of letters to type 90 characters per minute [Chen X., 2015: E6058-E6067], a recently decoded speech attempt has resulted in onscreen rate of 150 words per minute. This example gives an idea of how quickly we can have a seamless direct brain-computer link. However, compared to understanding, texting or dictation is a fragmented capability. The efforts to reconstruct perceptive experience, memories, emotions and conceptual thinking from decoded neural patterns foreshadow radically higher BCI throughput.

Table 1. Cortical Labs key features

Feature	Description
Biologically plausible neural networks	Research and simulation of neural network structure and behavior in animal/ human brain for realistic AI design
Neuromorphic chips	Designing specific neuromorphic processors (Anthropic Neural Computers, ANC) optimized to launch such biologically plausible networks
General artificial intelligence	Models for general intelligence rather than specific tasks able to solve a wide range of cognitive problems just like man

Neuron visualization achievements set the stage for developing a capability to *read out* thoughts. Kernel's brain-chip interface attempts to capture hippocampus activities and to externalize memories [Hassabis D., 2021: 493–498]. Facebook's sensory headband aims to decode coded speech for augmented reality devices. Neuralink's 3000+ channel readouts have enabled real-time forecasting of limb movements in primates [Musk N., 2019]. Simultaneous innovations in stimulation technologies allow to *record* sensory and cognitive data. Examples of bidirectional communications are the experience induced in patients by temporal lobe stimulation and optogenetic induction in rodents.

Current developments also hold a promise of remote, wireless and possibly covert capabilities. Ultrasound neuromodulation can transcranially influence brain areas without a need for implants [Menz M., 2021: 2919-2933] while EEG biometry is capable of discreet user authentication [Sun Y., 2020: 31005]. The emerging reconfigurable neural sensors can detect chronic states of the brain [Seo D., 2020: 1-17]. Portability also allows to track users in different environments, for example, as envisaged in Facebook's VR BCI. Miniaturization allows to embed applications as in Smart Stent's neurovascular interface (Table 2). The said trajectories are fraught with far-reaching implications affecting cognition, identity, privacy, behavior, justice and social cohesion, all of which require further discussion.

Table 2. Smart Stent key functions

Function	Description
Minimally invasive implantation	The device is to be implanted into brain blood vessels transvascularily without a need for open brain surgery
Brain activity recording	The device is to record signals from brain areas responsible for motion control
Auxiliary device control	Decoded neural data are to be used for control of external robotic systems, exoskeletons, other rehabilitation devices

1.2. Classification of the Key Threats to Rights and Liberties

In absence of proper supervision, the above adaptive capabilities will create major threats classified by this study in light of governance priorities. These threats include unauthorized data access, manipulative and discriminative applications, non-transparency and non-accountable commercialization.

Once ubiquitous, personal data collection creates a new risk of identity theft, emotional manipulations and discriminative refusal of opportunities. In fact, EEG biometry has been shown to distinctly identify people, with psychological profiling becoming a new application in its own right, only to result in unauthorized access or tracking. Selective data filtration based on decoded neural states will amount to manipulative censorship. In absence of proper checks, the identification of neural markers of risk, disease or demographic profile is a signal for predatory exclusion from service, a cognitive equivalent of genetic discrimination.

Direct neuromodulation is fraught with a number of extra risks of behavior compromise. Animal studies have shown that induced stimuli will cause specific behavior — for instance, one study [Adamantidis A., 2015: 420-424] points out to the potential for unauthorized influence.

Sensory manipulations can create neural evidence in favor of invalid assertions or sow discord by distorting perception and memories in event witnesses. These capabilities red-flag a forced and deceitful use to call for an extra level of control. They highlight the importance of the boundary between therapeutic applications for improved well-being and those that do not respect the autonomy of individuals.

1.3. Weak Security Provisions

Experiments with simple methodologies have demonstrated a potential for embedding malware into the brain via consumer headsets, neural signal spoofing and EEG data theft [Sun Y., 2020: 310]. With direct access to executive functions, BCI 5.0 will multiply the potential power of ransomware. Compromises between encrypting neural data and allowing crucial application are still an open question. Moreover, non-clinical BCI applications bypass supervisory standards for health devices despite health risks caused by direct brain stimulation. Such vulnerabilities highlight the need for special guarantees.

Non-transparency of business applications is itself a cause of concern since the incentives of dominant companies will often conflict with user well-being. In fact, the past study of Facebook's emotional contamination is an illustration of the willingness to discreetly manipulate users. With an opportunity to access or impact individual thoughts and feelings, behavior could become subject to unprecedented threats of persuasive power facilitated by the absence of guaranteed transparency and democratic supervision. With such applications deployed on a massive scale, proactive governance to prevent harm is a matter of priority.

2. Legal Regulation of BCI and its Constraints

2.1. Current Regulatory Principles Adopted Globally for Innovative Technologies

A policy framework for protecting individual rights from the emerging BCI applications should rely on the key governance principles designed for the existing technologies capable of affecting the brain.

The discussed international standards show a commitment to human rights, with a majority guided by democratic considerations in adopting the technologies that have an impact on human life. The declared principles of international law include the universal declaration on bioethics and human rights that asserts human dignity, autonomy and consent in medical interventions on the brain. However, such declarations are devoid of mechanisms for enforcement which is left to the national law. Thus, the outcomes of protection will vary between jurisdictions.

Legal scholars believe direct access to thoughts to be sensitive enough to call for stricter supervision than is imposed on biometric and communication data. While some argue for applying restrictions only to ways of retrieving information outside human control, others are not as sure in respect of voluntary applications. Still others argue for control to maximize user autonomy over neural data flows. BCI also require informed consent with new designs that allow to use dynamically revocable and granular permissions.

In absence of specific rules applicable to BCI, some instructive precedents come from adjacent areas. For example, the law governing medical devices, human subject research and consumer goods offers comparative points of reference as for requirements to BCI system quality, safety and accountability. Protection of health data signals a need for cyber-security and access control policies to include, apart from openness and follow-up supervision of experiments to simulate high-risk BCI applications, advice on institutional bioethics. These mechanisms can be adapted to account for unique problems arising in BCI studies. Overall, the current framework is respectful of human dignity but also highlights awareness of the need for careful scrutiny in rapidly developing areas. Meanwhile, the current controls can only deal with new issues such as the constancy of access to thoughts, with a balance to be struck using the available principles as a backbone to provide special guarantees for BCI 5.0 capabilities.

2.2. Constraints of the Rules for BCI 5.0 Adoption

Making BCI 5.0 integration socially useful and respectful of rights requires governance adapted to new technological features. Conversely, the analysis shows constraints of direct application of the existing legal framework designed largely for biometric, communication and legacy computer technologies.

While intuitive logic assumes that access to thoughts requires higher levels of protection than those afforded to behavioral data, few of the existing regulatory differences will recognize this boundary.

As such, global data rules remain purely information-driven as they restrict the use of collected data. Real-time access to neural processes is out of scope of a vast majority of global data protection rules such as the General Data Protection Regulation (GDPR). Some persons believe it to be essentially a real-time access to another form of mental privacy that should be protected. There is a need for balance which would enable legitimate use of technologies without violating the boundaries of mental privacy.

The same ambiguity surrounds the concepts that define BCI admissibility. Freedom of cognitive improvement is a principle upheld by international policies, with coercive practices being forbidden. Meanwhile, even the legal definitions of coercion will normally revolve around obvious force or threat, only to exclude the opportunity for more delicate manipulations enabled by BCI. Therefore, a more nuanced governance should be established to distinguish applications for positive cognitive reinforcement from those that undermine mental integrity.

For example, the present-day rules will focus on illicit use or dissemination of information. BCI have exclusive access to thoughts even where ongoing recording is not assumed. Control of the actual real-time data collection is thus desirable due to implied sensitivity. An adequate way of protecting designed for BCI's constant neural access routes involves multi-level access control and revocable permissions, a deviation from a normal data protection framework.

Finally, sectoral regulation will often exclude consumer technologies even of high social impact, with higher standards applicable to medical equipment for restricted access to therapeutic devices. Once adopted, multi-level supervision for a balance between innovations and proportional control of high-risk applications can overcome this constraint. On the other hand, responsive governance is achieved by adapting some of the aspects such as tentative market overview and post-launch monitoring of BCI elaborations across all sectors.

2.3. Implications of Inadequate Legal Protection of Digital Rights

In absence of meaningful guarantees to match special capabilities enabled by BCI 5.0, the above categorized risks to individual rights become highly probable. Beyond breaches of neural privacy and actions as such, they threaten to routinely erode civil liberties as a whole.

What is the most disturbing, unregulated BCI commercialization can make normal the breaches of neural privacy that will be intuitively perceived as negative. Legitimizing such access, even to a minor extent, creates alarming preconditions for thought control and ideological coercion by authoritarian governments in the future. Moreover, if protection of civil liberties from violation is not there for too long, human rights will be threatened [Jobin A., 2019: 389–399]. Careful approach is urgently needed because the slope from benevolent to repressive use is slippery [Hildt E., 2021: 1–12].

Finally, it is decentralized technical design that offers a unique potential for upholding rights in the emerging sectors. With data access architectures broadly available across societies like social media previously, post-factum regulation is unlikely to rectify violations. Embedding the elements of security, protection and consent control into the technology itself means that protection will be there in the event of adaptation. Political and technical guarantees are joined to reliably secure the interests of individuals from the emerging threats.

A lack of security provisions in BCI 5.0 is threatening to make low cyber-security standards normal despite being dangerous for public well-being in a broad sense. Designs supporting transparency, access protection and audit control would create incentives for a cultural shift towards data management. The risk of neural data theft and compromised sovereignty is socially unacceptable: security and democratic supervision should become priority number one. Unprecedented risks arising from uncontrolled BCI commercialization coupled with constraints of the legacy political framework highlight an urgent need for innovative governance to protect individual rights to cognitive freedom.

3. Technological and Legal Safeguards for Protecting Digital Rights in the Context of BCI 5.0

3.1. Technical Guarantees for Better Security and Privacy in BCI 5.0

Apart from policies, technical principles of design and architecture can also provide ways for secure and ethical evolution of BCI 5.0 ecosystems respectful of human rights.

Federated learning enables collaborative model training on user data without exchanging the data themselves to preserve privacy. Thus, users can benefit from crowdsourcing applications while preventing exploitation of their neural patterns. Mixing proxy data via algorithm development methods such as differential privacy leaves less room for re-identification while providing insights. Access to insights for achieving improvement without damaging user privacy is one of technological pillars of an ethical BCI.

Another core safeguard involves encryption and control of protection in line with the standards of the Health Insurance Portability and Accountability Act for electronic health records, something that ensures security in preserving utility. For instance, selective disclosures such as cryptographic registration details to confirm identity attributes without revealing raw biometric data will protect user interests via approaches proposed by [Soares J., 2012: 149–155]. Encryption of high-density neural data flows is currently constrained by the level of computational overheads.

Blockchain architectures (decentralized ledger) will also support secure audit for access and permission management service under user control. Action support mechanisms in connected technologies point to smart contracts that ensure limited purpose and revocable data exchange by cryptographic consent tokens rather than unconditional access. It is a combination of computational law tools with adaptive policies that can provide robust protection of the rights.

Human-centric privacy, accountability, democratic supervision technologies are indispensable supplements to top-down regulation where individual interests and liberties are to be protected from the emerging threats. Multi-level governance will blend the strengths of these approaches in a way that securely expands the potential of socially useful innovations while containing risks generated by the emerging neurotechnologies.

3.2. Normative Minimum Viable Standards for BCI 5.0

Security and privacy will be critical for establishing basic regulatory norms and expectations that are important for meaningful provision of individual rights and interests of BCI system developers and users.

A vital prerequisite for ethical integration of BCI could be the assurance of improved protection of mental privacy beyond what applies to communication and even biometric data due to special sensitivity of this issue. These legal definitions are supposed to prevent real-time access to neural processes, not only permanent recording. While a need to ensure lawful applications requires nuanced approaches without total prohibitions, it also requires to avoid uncontrolled distribution.

This translates into a higher denial threshold before neural data could be collected or used in consumer applications, something really in line with medical ethics and proportional protection. In particular, consent-giving via multi-factor authentication for daily use or passive monitoring assumes a higher threshold than one-time approvals now predominant in digital systems. Dynamic revocation and granular permissions will additionally secure user actions. This will put the burden on the developer who should substantiate the need for access.

Technological protection is another pillar. The requirements modeled upon HIPAA security standards — those for tracking, logging and attempting to prevent healthcare data breaches — provide for accountability via data encryption, access control, audit and a lot more in fighting abuse and cyber-threats (Fig. 1).

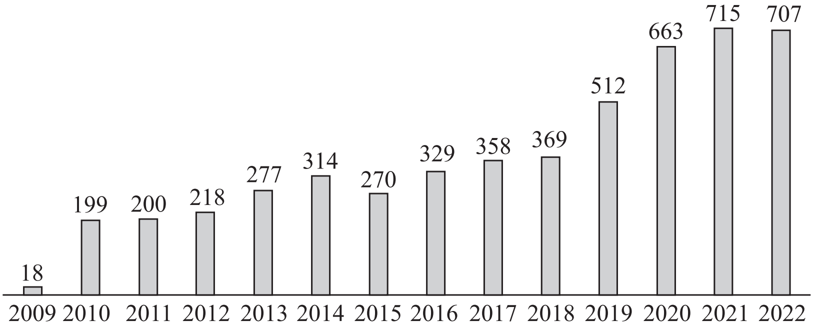

Fig. 1. Healthcare data breaches (reported by HIPAA, 2009–2022)

Federated analytics, differential privacy are some of the ways to maximize utility without harm to user interests. Security provisions designed for BCI threats ensure continuous protection along with applications.

Finally, the development of responsibility and compensation arrangements reflects recognition of the fact that some of the emerging technologies will cause harm even despite due care. Well-informed ways for compensation of damage, flexibility to adapt to ever evolving stock of impact evidence and participatory mechanisms in supervision regimes could ensure accountability. In combination, such basic reasonable guarantees strike a balance between unfettered innovations and provision of necessary safeguards against BCI pitfalls.

3.3. Material Amendments to the Data Protection act in Light of BCI-related Challenges

Full drafting of policies and rules for disruptive adoption of BCI requires to revisit the existing policy framework designed largely in response to technologies of the past. Given below are specific amendments to support priority reforms for more comprehensive rights protection in light of the analyzed risks.

While the effective law has a strong focus on regulating how the collected information is used, real-time access to thoughts requires better protection at the very initial level because sensitivity passes by the authorization and use restriction requirements [Ienca M., Haselager P., 2016: 117–119]. Provisions that restrict unwarranted collection of neural data combined with the existing rules of use will provide consistent protection.

Narrow definitions of coercion and inappropriate influence in regulating the persuasive technologies should be expanded to account for intricacies in BCI. The evidence that neural processes can be manipulated to induce relationship, behavior and memories without any obvious force or deceit means that governance should counter such influences on psychic integrity.

Moreover, customized supervision mechanisms will address the problem of combining medical and consumer uses of BCI and will balance innovations with supervision in proportion to the identified risks. The rules may require high-risk interventions to be subject to security checks in the same way as pharmaceuticals or medical devices while transparency provisions target the applications designed for consumers. Thus, nuanced models can enable the consideration of specific risk profiles.

Responsive governance is possible via the expansion of rights and methods of compensation for damage combined with flexible liability funds compensating documented harm. With such arrangements, mandatory insurance of developers from verifiable abuse will contain risks while allowing unfettered innovations by avoiding preventive restrictions, and will make these emerging laws compatible with BCI realities.

3.4. Codifying Rights and Restrictions for BCI 5.0 via Computational Law

Apart from policies, there is a good chance to embed the rules of legitimate use and protection of rights into technological architectures via computational law. Smart contracts will codify ethics embedded into technologies to enable granular, dynamic and transparent consent management. Users can preset access restrictions to be automatically enforced to prevent any future abuse. A certain revocation of consent can trigger guaranteed cascade deletion of data. It is these computational iterations of law that that contribute to fail-free protection.

Such applications also allow real algorithmic output-related events to control codified supervision and regulation. Third-party audits certified to approve sound data processing practices could automatically extend operating licenses. Problem reports by representative civil juries can trigger inquiry and rectification cascades. The final goal is to embed social checks and balances via computational law and to uphold accountability.

Overall, careful integration of legal principles directly into technological architectures in an inventive way allows to preempt risks while ensuring unfettered innovation. Rather than responding by restrictions, computational law options offer proactive protection of individual rights and interests holding an enormous promise for ethical integration with neurotechnologies.

3.5. Automating Protection of Digital Rights Using Smart Contracts and Oracle AI Agents

A very promising area for drafting and enforcing policies via the emerging technologies of computational law — as in smart contracts, decentralized apps and tokenized consent systems — is automated enforcement and monitoring of policies proposed for protection of individual rights in the context of BCI.

Dynamic permission tokens can codify the above proposed type of granular consent policies directly into access control infrastructure via smart contracts. Users could manage such permissions on their own, for instance, by deleting EEG data exchange for business while maintaining all access data for health purposes. Pre-programmed rules can trigger the necessary deletion of data when the purpose expires. General consent management will also avoid any dependence on external coercion.

Meanwhile, AI agents trained as LegalTech applications can algorithmically identify breaches of codified rights to protection by system logs and user reports. As an illustration, applications could note unauthorized passive neural monitoring or flag business applications failing a risk assessment. To provide quick protection, applications could automatically generate warnings, escalate to human review and technically disable systems when breaches exceed probative thresholds.

Wider/decentralized autonomous organizations where users manage policies on their own to balance innovation risks on a peer-to-peer basis rather than under a formal corporate order also offer promising ways to uphold rights. Such codified iterations of legal principles allow to go beyond upgrading restrictions on the use of technologies to a technology designed for mutually conceived supervision, with potential benefits explored in parallel with policy development.

Overall, the proposed guarantees, once implemented directly in the code, can sustainably ensure that the layer of rights is resistant to regulatory destruction. The technological architectures that embed supervision and balance the incentives for innovation with social well-being can complement some key reforms on the way to the ethical neurotechnological future. This will require intensive multidisciplinary collaboration all along the way — from conceptualization to implementation and testing.

4. Liability and BCI-Related Dispute Resolution

4.1. Methods to Demonstrate Claims for Compensation and to Settle Disputes in the Event of Unauthorized Use

In the pursuit of risk preemption, good governance will also assume setting up specific mechanisms for rectification in case of verifiable damage that can arise even with strict guarantees in place.

Encrypted logging and watermarking methods allow to identify a single path of traceable evidence of unauthorized use thus ensuring restitution. For example, users can register personal EEG signatures to allow for attribution as soon as such activity is accessible or synthesized by unauthorized parties. Embedded digital watermarks allow to check neural data for commercial appropriation and licensing breaches. Any abuse should be proved with inalterable records for possible further action.

Proportional liability funds supported by mandatory security deposits rather than penalties or criminalization will facilitate settlement. Claims can be processed and compensation distributed by democratically governed independent supervisory boards with civil membership.

In other words, the availability of probative evidence resulting from novel judicial methods along with channels for compensation will make it possible to use non-punitive but rectifying mechanisms to uphold justice. The regulatory design's focus on direct mitigation of damage rather than on preventive restriction can bring benefits while securing reliable guarantees. Technological and political synergies can provide a robust protection of individual rights.

4.2. Current Regime for Distribution of Liability for Damage

hile striving to minimize unnecessary damage, a realistic assessment will recognize that unintended effects from rapid progress of the emerging technologies such as BCI 5.0 are inevitable. Applying the existing legal principles with regard to distribution of liability for so-called "unintended but inevitable" harm assumes a point of departure where there is no provable malice of any kind.

The effective regimes for products admit different distributions of liability between producers and consumers based on the analysis of due care on both sides in light of the reasonable care standard [Miller J., Goldberg R., 2004: 149-155]. Producers adhering to the acknowledged best practices would face limited liability for unforeseen errors. However, consumers in violation of the due care obligation (such as failing to turn on security functions) would face the distribution of liability within this extent.

The application of similar principles to balance accountability, innovation and precaution in BCI use would uphold equity. Scenarios of unintended harm via compromised devices or careless use of functions would result in a mixed model. On the contrary, where security is weak due to negligence or deployment of risky unauthorized applications, it would be fully justifiable to impose stricter liability on producers. Overall, the existing nuanced framework offer some initial guidance on the arising problem.

However, new technological spaces also require to consider extended social liability models for aggregate public effects. Isolated disputes clearly inadequately capture the general implications of harm as BCI 5.0 is promising to be profoundly transformative both on individual and collective scale. Going deep into integrated compensation, rehabilitation and recovery systems to achieve real social outcomes provides the best opportunity to maximize the protection of rights. This is worthy of more careful scrutiny.

4.3. The Importance of Establishing Guilt in Criminal Activities with Compromised BCI Systems

While the previous sections deal with mitigating unintended harm, it would be realistic to discuss pragmatic adversarial settings in the face of quasi-dualistic nature of integrated neurotechnologies.

Seamless BCI 5.0 integration obfuscates agency attribution and, therefore, guilt for criminal action in systems made vulnerable by malignant actors. Where the executive function control was seized, it will be hard to identify with sufficient certainty whether the criminal intrusion was committed by the user or hackers. If the guilt cannot be ascribed, fair responses are difficult.

But arbitrary attribution of fault will punish the victims of manipulation. Too much zealous prosecution will also suppress incentives to report and disclose the information required for better protection. However, due to ambiguity, universal immunity escapes accounting, only to allow exploitation. On should proceed with care in these dilemmas.

Technological options such as blockchain-based data recorders, access and threat logs are potential sources of evidence to identify liability [Kshetri N., 2024: 117–119]. Behavioral forensics would establish a deviation from personal baseline as indicative of compromise. Still less than perfect reconstruction is a reality as to the existence of a barrier to satisfy probative thresholds. There is a special need to develop verifiable diagnostics [Froomkin A., 2020: 513].

This broad problem underlines tension between justice, freedom and security due to the risks and ambiguities arising from BCI. But a repressive bend would be as much dangerous as reckless indulgence. Governance projecting the importance of sincere strife to the truth and reconciliation leads to socially approved outcomes. A multidisciplinary analysis that necessarily follows will discuss ways to uphold ethics.

4.4. Call for an Ethics Charter to Prevent Unauthorized Use

Interrelated risks in all these analyses point to the development of a culture of responsibility to secure socially useful future outcomes.

One such setup would include the principles of necessity and proportionality just as those of consent and privacy, transparency and accounting, harmlessness via inclusive discussion. It would define the duties of producers that consider social aspects of effects, characterize risks, embed protection systems into technological design, provide remedies in the event of harm, and discourage harmful business models as much as currently possible. The relevant duties of users would include bona fide consent-giving, problem and unauthorized use reporting, and provision of feedback for system improvement.

Charters endorsed by producers and representative consumer groups define voluntary but mutually binding obligations in accord with the proposed regulatory guarantees. They carry non-punitive signals beneficial for public confidence and create provisions. While the framework will need an upgrade in view of the lessons learned and expectations, the original pacts will lay the brickwork for subsequent collaboration.

Despite inherent risks due to rapid dissemination, charters embodying ethics through corporate responsibilities achieve responsiveness and self-regulation. They extend powers to stakeholders rather than create isolated authoritarian restrictions. While value-based partnerships cannot do without formal policies, they have been found to meaningfully uphold secure and equitable innovation paths [Yuste R. et al., 2017: 159–163]. Science, politics, business and society — all should join forces to secure this obligation.

5. Import of Findings and Their Implications

The study has endeavored an in-depth analysis of the emerging capabilities and constraints of BCI 5.0 to design policies and technical interventions aimed at protecting user rights. The above sections contain a synthesis of robust technical assessment, comparative policy analysis, predictive risk modeling and the relevant proposals for governance.

Predictive analyses based on the experience of related sectors confirm the emerging threats created by commercialization unbridled by incentives that agree with user well-being. They highlight how governance should discourage antisocial uses before their dissemination is deeply rooted. Nevertheless, excessive care is fraught with the risk of containing useful development. Navigating through these competing tensions requires nuanced, adaptive and multimodal interventions that were proposed here.

Drafting minimum viable guarantees and amendments to upgrade protective framework and tools for application of computational law provides some of the ways to maximize opportunities for securing rights.

Embedding ethical practices directly into technological architectures and organizational models reliably secures protective capabilities — often beyond what is achievable by the external regulation [Frolova E., Lesiv B., 2024: 15]. Synthetic recommendations on technological, political and cultural interventions provide comprehensive guidance to implement positive future outcomes.

Overall, this integrated technical and social analysis presents key ideas and tools to inform the efforts to prepare stakeholders for forthcoming dissemination of neurotechnologies. As such, this is an enormous step towards human improvement that needs to be re-formatted for preemptive governance in going forward towards equitable innovation to secure beneficial outcomes across society.

6. Current Analysis Constraints

While this study achieves an extensive range through a synthesis of social science, engineering, legal and ethical perspectives, its findings should be treated with care recognizing inherent constraints that stipulate their use and identify steps to follow.

As the most general point, all analyses are underpinned by efforts to predict what is likely to occur in the near future but is still in the making. Though they are based on demonstrated prototypes, the exact functionality that leaves room for risk is an open empirical question. Real practices may deviate from forecasts in ways that cannot be foreseen.

Moreover, complex social and technical phenomena have evolved due to unpredictable shared constitution between technological and social entities [Volos A., 2024: 90]. Statistical analyses are in peril of neglecting the emerging future outcomes with new opportunities inducing unforeseen uses, adaptations and harm in need of permanent reassessment; therefore, one should monitor the ongoing co-evolution.

In this way, the discussed study provides a necessary basis for multiple paths via prospects and risks of a rapid launch of integrated neurotechnologies. Wise use, however, is necessary where foresight has reached its limits. Ongoing reassessment and understanding of the arising divergence is needed to stay on track.

The current findings indicate a number of key pathways for further research and studies of the questions that are left open.

Technical studies of analytics for preserving privacy of high-density neural data flows would finally enable progress in the proposed guarantees, with better consistency between non-invasive BCI and implanted systems to improve the diagnostic and therapeutic utility. Moreover, studies of user interfaces for effective consent and understanding of risks are crucial for creating human-centric designs.

Finally, studies of transition management approaches that link the upcoming business realities with long-term aspirations will help maintain pragmatic focus. For example, studies of voluntary sectoral ethics charters can provide insights into the best practices for early efforts. Practical testing of the proposed computational law tools assumes checking their efficiency in the real world. Such empirical steps to translate principles into reality remain an important complement of conceptual policy development.

These pathways to perfection demonstrate how responsible BCI innovations could be maximized. Taken collectively, technical, sociological and philosophical understanding of success to be achieved can provide the basis for interaction with already occurring fundamental shifts and for joint projecting of equitable outcomes in the future. The discussed study provides a tentative structured outline for such urgent joint endeavors.

Aggregating the identified opportunities, gaps and risks results in a balanced set of political, technical and cultural recommendations that allow to responsibly steer the implementation of BCI 5.0 capabilities while securing social values and rights. In particular, it is recommended to:

design in light of the above discussion of opportunities, gaps and risks a multi-level adaptive policy recognizing the unique risk-benefit compromises in BCI applications while avoiding universal governance;

require higher consent modeled on medical ethics for access to neural data due to sensitivity of the issue;

draft technical standards and design incentives for better security and privacy, and for user supervision opportunities;

provide proportional mechanisms of accountability and compensation for verifiable but unintended harm;

encourage civil participatory supervision and multidisciplinary expert contribution to governance;

embed ethical principles and protection directly into technologies via computational law wherever possible;

encourage collaborative sectoral self-governance via associations and voluntarily adopted ethics charters;

invest into multidisciplinary predictive studies to inform the emerging policies;

provide for more civil engagement and participative innovation design in agreement with social values;

achieve international consensus on fundamental principles with room left for regulatory diversity.

With such holistic, adaptive, human-centric governance, the transformative potential of BCI 5.0 could be equitably and safely geared to serve the purpose of prosperity for all. Sustainable, inclusive public discussion combined with bona fide policy design can thus channel these historical opportunities towards moral goals.

Conclusion

The study is an attempt of multidisciplinary research of the emerging BCI 5.0 systems to propose special governance arrangements for balancing capabilities brought by innovation with preventive rights protection.

It provides an overview of the current achievements in BCI that are rapidly approaching ubiquitous and seamless man-computer integration for unconstrained communication, control of environment, extended memory and a number of other improvements potentially within reach. They are also fraught with risks of ongoing neural data monitoring, hostile manipulations, compromised security and other breaches in absence of appropriate guarantees.

A comparative overview was conducted to understand constraints for direct application of the existing legal framework for privacy, security and protection of users in adequately managing BCI capabilities. Regulatory gaps pending removal were identified in respect of real-time data access and use, updated definitions of mental privacy and especially adaptive approaches to monitoring. An uncontrolled progress of these technologies can mean normalization of such invasive practices.

Predictive modeling based on what has been learned from the related sectors of persuasive computing, biometry and personalized medicine highlights the likely risks of poorly coordinated economic incentives and inadequate guarantees. Thus, innovative governance will be required to avoid potential threat for individual and collective rights.

A synthesized structure of specialized guiding principles currently allows to design a road map for bidirectional tracing of political and technical paths towards preservation of rights and achievement of socially useful outcomes. Stakeholders could systematically implement the recommendations via the following practical steps:

Policymakers could continue the dynamic upgrade of mental privacy laws to regulate real-time access, address supervisory gaps and tighten the requirements to user safety using the proposed multi-level risk model. A phased introduction can enable iterative improvements.

This could include the implementation of privacy preservation architecture, ethical risks assessment and transparency obligations, and even the development of the best practices and supervisory bodies for the sector as a whole — everything that can promote accountability. Users would thus have a voice in respect of security provisions, informed consent, duty of care in the process of use, expression of concern and request for damage compensation mechanisms for independent agency in BCI device integration.

A combined implementation of such recommendations can ensure equitable achievement of many critical advantages.

Acting on the proposed guiding principles could catalyze ethical innovation ecosystems in BCI in the interest of scientific community, businesses, regulatory bodies and the public at large.

A focus on privacy and security can expand the range of BCI research by enhancing user confidence in secure neural data exchange. Introducing the ethical review and supervision mechanisms will improve the conduct of research.

Responsible innovative channels will create long-term social and regulatory confidence crucial for sustainable success. Voluntary self-regulation will preempt restrictive policies that hold back progress.

For the public at large, innovative trajectories focused on social values and rights will generate more options for useful access. Channels for monitoring and damage compensation create ways for participation. Overall, general responsibility can create a driver for significant progress in the living standards of population.

A paradigm shift for ethical innovative BCI ecosystems should be realized by all stakeholders in a coordinated way.

Policymakers should promote multi-level regulatory models to balance unfettered innovations with supervision of high-risk applications based on the established principles; propose incentives to design privacy preserving architectures; systematically engage expert community and civil society for contribution to the development of specialized governance; and invest into foresight to manage adaptation.

Developers should embed transparency, auditability, secure design and user-led supervision into block chain design and development options; adopt the practices of ethical risk assessment and monitoring; take part in promotion of the best practices and professional association ethical standards.

Users should be allowed to provide informed consent for BCI use including privacy provisions. They should take precautions for use and monitoring; provide feedback and report problems to help improve systems; demand efficient claim processing mechanisms.

Researchers should study social, ethical and legal implications of BCI use in a wide range of sectors. They should explore practical ways to implement the proposed guarantees and guiding principles; provide inclusive discussions and participatory supervision mechanisms.

Civil interest groups can monitor BCI achievements and commercialization, raise issues and advocate policies and business models that serve the interests of society.

This could include civil society participation in responsible innovations. BCI 5.0 prospects are a cause of surprise and concern. Nevertheless, equitable and safe development respectful of rights can bring promising future outcomes to reinforce human potential in all communities. Let out collective action rise to the challenge with urgency and wisdom required by the current moment.

References

1. Adamantidis A. et al. (2007) Neural substrates of awakening probed with optogenetic control of hypocretin neurons. *Nature*, 450 (7168), pp. 420–424.

2. Allen C. et al. (2020) Artificial morality: Top-down, bottom-up, and hybrid approaches. *Ethics and Information Technology*, vol. 22, no.3, pp.149–155.

3. Anumanchipalli G. et al. (2019) Speech synthesis from neural decoding of spoken sentences. *Nature*, 568 (7753), pp. 493–498.

4. Bublitz J. C. (2013) My mind is mine?! Cognitive liberty as a legal concept. In: Freedom of the Mind. Baden-Baden: Nomos, pp. 233–264.

5. Burwell S. et al. (2017) Ethical aspects of brain computer interfaces: a scoping review. *BMC Medical Ethics*, vol. 18, no.1, pp. 1–12.

6. Chen X. et al. (2015) High-speed spelling with a noninvasive brain–computer interface. *Proceedings of National Academy of Sciences,* vol.112, pp. E6058–E6067.

7. Das D.M. et al. (2021) Brain-computer interface: Advancement and challenges. *Sensors*, no. 17, p. 5746. https://doi.org/10.3390/s21175746

8. Frolova E., Lesiv B. (2024) Sources and Forms of Law: a Modern View on Basic Theoretical Provisions. *Law*. *Journal* of *the Higher School of Economics*, vol. 17, no. 1, pp. 4–39. https://doi.org/10.17323/2072-8166.2024.1.4.39 (in Russ.)

9. Froomkin A.M. (2020). Regulating mass surveillance as privacy pollution: Learning from environmental impact statements. *University of Illinois Law Review,* no. 2, pp. 513–572.

10. Gulyamov S.S., Rodionov A.A., Rustambekov I.R. and Yakubov A.N. (2023) The Growing Significance of Cyber Law Professionals in Higher Education: Effective Learning Strategies and Innovative Approaches. International Conference on Technology Enhanced Learning in Higher Education, pp. 117–119, doi: 10.1109/TELE58910.2023.10184186. https://ieeexplore.ieee.org/document/10184186

11. Hassabis D. et al. (2021) Neuroscience-inspired artificial intelligence. *Neuron*, no. 3, pp. 493–498.

12. Hildt E. (2021) Multi-person brain-to-brain interfaces: Ethical considerations. *Frontiers in Neuroscience*, no. 15, pp. 1–12.

13. Hiremath S. et al. (2015) Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare. In: 2015 International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare through Innovations in Mobile and Wireless Technologies, pp. 304–307.

14. Ienca M., Haselager P. (2016) Hacking the brain: Brain-computer interfacing technology and the ethics of neurosecurity. *Ethics and Information Technology*, vol.18, no. 2, pp.117–119.

15. Jasanoff S. (ed.) (2015) Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power. Chicago: University Press, 360 p.

16. Jobin A., Ienca M. (2019) Global landscape of AI ethics guidelines. *Nature Machine Intelligence*, vol. 1, no.9, pp. 389–399.

17. Kramer A. et al. (2014) Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of National Academy of Sciences,* vol. 111, pp. 8788–8790.

18. Kshetri N. et al. (2024) Blockchain technology for cyber defense, cybersecurity, and countermeasures: Techniques, solutions, and applications. https://doi.org/10.1201/9781003449515

19. Lotte F. et al. (2018) A review of classification algorithms for EEG-based brain–computer interfaces: a 10 year update. *Journal of Neural Engineering*, vol. 15, no. 3, p. 031005.

20. Menz M., Oralkan O. et al. (2019) Precise neural stimulation in the retina using focused ultrasound. *Journal of Neuroscience*, vol. 39, no.15, pp. 2919–2933.

21. Miller J., Goldberg R. (2004) *Product liability*. Oxford: University Press, 386 p.

22. Musk N. (2019) An integrated brain-machine interface platform with thousands of channels. *Journal of Medical Internet Research, vol.* 23, no. 10, p. e30903.

23. Naseer N. (2015) NIRS-based brain-computer interfaces: a review. *Frontiers in human neuroscience,* no. 9, p. 3.

24. Reijers W., O'Brolcháin F. (2018) Governance in blockchain technologies & social contract theories. *Ledger*, no. 3, pp. 1–17.

25. Sample M., Bauer Z. (2021) Brain-computer interfaces and personhood: Interdisciplinary deliberations. *Cambridge Quarterly of Healthcare Ethics*, vol. 30, no.1, pp. 157–169.

26. Soares J. et al. (2012) Privacy-preserving attribute-based encryption for brain-computer interfaces. *Journal of Medical Systems*, vol. 36, no.1, pp. 149–155.

27. Sun Y., Zhang H. et al. (2020) EEG-based biometric authentication: A comprehensive survey. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 2, no. 4, pp. 310–324.

28. Volos A. (2024) Concept of Weak Party in Civil Matter in Context of Digitalization. *Law. Journal of the Higher School of Economics,* vol. 17, no. 3, pp. 84–105. https://doi.org/10.17323/2072-8166.2024.3.84.105 (in Russ.)

29. Yeung K. (2021) Algorithmic regulation: a critical interrogation. *Regulation* & *Governance*, vol. 12, no. 4, pp. 505–523.

30. Yuste R. et al. (2017) Four ethical priorities for neurotechnologies and AI. *Nature*, 551(7679), pp.159–163.

Information about the author:

S.S. Gulyamov — Doctor of Sciences (Law), Professor.

The article was submitted to editorial office 28.10.2024; approved after reviewing 14.01.2025; accepted for publication 18.02.2025.