Revisiting the Concept of Victimization in Cybercrimes Against Neural Data: From Physical Harm to the Violation of the Victim's Mental Integrity

1. Hamzeh Hamdami Khotbeh Sara: Department of Law, Sav.C., Islamic Azad University, Saveh, Iran
2. Hamid Shakeri*: Department of Law, Das.C., Islamic Azad University, Borazjan, Iran
3. Mahmoud Habibitabar: Department of Law, Sav.C., Islamic Azad University, Saveh, Iran

*Correspondence: h.shakeri8998@iau.ac.ir

Abstract

The expansion of neurotechnologies and their integration with artificial intelligence systems have transformed neural data into one of the most sensitive and personal categories of human data—data capable of revealing mental states, preferences, emotions, and even individual decision-making patterns. This transformation has given rise to a novel category of cybercrimes that extend victimization beyond the realm of physical and data-related harm into the domain of "mental integrity" and "cognitive autonomy." The present study aims to reconceptualize victimization in cybercrimes targeting neural data and to elucidate the emerging dimensions of victim vulnerability. It employs a descriptive–analytical method and adopts an interdisciplinary approach drawing on criminal law, criminology, neuroscience, and technology ethics. The findings indicate that neurocybercrimes—including theft, manipulation, decoding, or unauthorized surveillance of neural data—generate a multilayered form of victimization encompassing physical, data-related, cognitive, and existential harms. These harms manifest particularly through violations of cognitive privacy and intrusions upon the psychological integrity of the victim. The results further demonstrate that existing criminal law frameworks are insufficient to adequately protect victims against such offenses, necessitating a redefinition of core concepts such as "harm," "integrity," and "privacy" in light of cognitive rights and principles safeguarding mental integrity.

Keywords: Neural Data; Cybercrime; Cognitive Victimization; Mental Integrity; Cognitive Privacy; Cognitive Autonomy; Neurotechnology

Received: 01 January 2026
Revised: 01 May 2026
Accepted: 05 May 2026
Published: 01 July 2026

Copyright: © 2026 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Citation: Hamdami Khotbeh Sara, H., Shakeri, H., & Habibitabar, M. (2026). Revisiting the Concept of Victimization in Cybercrimes Against Neural Data: From Physical Harm to the Violation of the Victim's Mental Integrity. *Legal Studies in Digital Age,* 5(4), 1-14.

1. Introduction

The rapid transformations of digital technologies in recent decades have disrupted the traditional boundaries between humans and machines in an unprecedented manner. One of the most important manifestations of this transformation is the emergence of neurotechnologies and brain–computer interfaces, which have made it possible to record, analyze, and even interpret human neural activity. Neural data, as a direct reflection of an individual's mental, emotional, cognitive, and decision-

making states, have now become one of the most valuable and, at the same time, most vulnerable categories of human data. These data not only reveal an individual's biological information but may also penetrate deeper layers of mental identity and cognitive privacy; layers that, until recently, were essentially beyond the reach of technology and, consequently, outside the domain of criminal law.

In this context, a new form of cybercrime is emerging that directly targets neural data. These crimes, ranging from the theft and disclosure of neural data to the manipulation, decoding, or unauthorized surveillance of brain activity, create a form of victimization that cannot be explained through classical patterns of vulnerability in criminal law. Whereas victimization was previously defined mainly in terms of physical, financial, or psychological harm, we are now confronted with a phenomenon that can impair an individual's "mental integrity" and "cognitive autonomy," matters that have received limited attention in legal and criminological literature.

On the other hand, recent advances in artificial intelligence and deep learning have made it possible to decode neural patterns and reconstruct mental images or emotional states. This has rendered the boundary between "privacy" and "cognitive privacy" highly ambiguous and has raised fundamental questions about the limits of criminal-law protection of the human mind. Can an intrusion into neural data be regarded as a form of violation of psychological integrity? Is cognitive manipulation an instance of criminally relevant harm? More importantly, are existing legal systems capable of responding to this type of victimization?

By raising these questions, the present study seeks to revisit the concept of victimization in cybercrimes against neural data. Using an interdisciplinary approach and drawing on findings from criminal law, criminology, neuroscience, and technology ethics, this study attempts to explain the emerging dimensions of victim vulnerability in the age of neurotechnology and to show why traditional criminal-law frameworks are insufficient for addressing this phenomenon. Ultimately, the article will present a conceptual framework for redefining victimization and for providing the theoretical foundations necessary for the criminal-law protection of "mental integrity."

2. Neural Data and Their Nature

Recent developments in neurotechnology and its integration with artificial intelligence systems have posed serious challenges to fundamental concepts in criminal law and criminology. Neural data, as the direct product of brain activity, possess a nature that distinguishes them from other biological and digital data. These data can reveal an individual's emotional states, cognitive processes, preferences, intentions, and even decision-making patterns, which has led scholars in neuroscience and technology ethics to describe them as "the most sensitive human data" (Farahany, 2023). Accordingly, any unauthorized access to these data may lead to the violation of cognitive privacy, the weakening of mental autonomy, and an intrusion upon the individual's psychological integrity. Unlike biological data such as DNA or fingerprints, neural data do not merely indicate a person's physical identity; rather, they are directly connected to mental identity. Ienca and Andorno emphasize that neural data are a "direct window into the human mind" and therefore require a level of legal protection that goes beyond ordinary protections for personal data (Ienca & Andorno, 2017). These characteristics have also led international organizations to stress the need to establish new frameworks for the protection of neural data (Oecd, 2019; Unesco, 2021).

Technological advances in brain–computer interfaces and deep learning algorithms have made it possible to record, analyze, and even reconstruct neural patterns. Modern technologies can reconstruct mental images, emotional states, and even individual intentions with considerable accuracy. In addition to their medical and rehabilitative applications, these capabilities have paved the way for the emergence of a new category of cybercrimes that directly target the human mind (Yuste, 2017).

In classical criminology, victimization was mainly defined in terms of physical, financial, or psychological harm. However, the emergence of neurocybercrimes has shown that this classification is no longer adequate. Intrusion into neural data can create a form of "cognitive victimization," a concept introduced in the literature on neuroethics and cognitive rights that refers to harms directly inflicted upon an individual's mental and cognitive processes (Ienca, 2021). This type of victimization does not arise from traumatic experiences but from the direct manipulation, extraction, or analysis of mental data.

Neurocybercrimes include the theft of neural data, manipulation of neural patterns, unauthorized decoding of thoughts, cognitive surveillance, and cognitive imposition. These crimes may lead to the loss of mental control, threats to free will, harm to psychological identity, and violation of mental integrity. Cognitive manipulation can threaten the deepest layers of human

autonomy and should therefore be recognized as an independent form of criminal harm (Farahany, 2023). In this regard, the concept of "mental integrity" has been introduced in recent years as one of the cognitive rights. This right is defined as the protection of the unity and independence of mental processes. Intrusion into neural data, especially through artificial-intelligence-based technologies, can seriously violate this right. For this reason, many scholars argue that the criminal-law protection of mental integrity must be regarded as one of the priorities of criminal law in the age of neurotechnology (Greely, 2021). Overall, the theoretical and conceptual foundations examined here show that neural data have a unique nature and that neurocybercrimes can result in cognitive victimization and the violation of mental integrity. These features highlight the need to reconsider traditional concepts of victimization and to develop new frameworks for the criminal-law protection of cognitive privacy.

2.1. Definition of Neural Data

Neural data refer to a set of signals, patterns of electrical activity, changes in cerebral blood flow, and information extracted from cognitive processes that are obtained through various neuroscience tools. Unlike biological or digital data, these data do not merely indicate an individual's physical condition; rather, they directly reflect mental states, emotions, intentions, preferences, and decision-making processes. In other words, neural data are regarded as a "window into the mind" and can reveal an individual's cognitive and emotional structures. Neuroscience scholars have emphasized that, due to their cognitive nature, neural data are the most sensitive type of data in the age of emerging technologies, and any unauthorized access to them may have profound and irreversible consequences (Ienca & Andorno, 2017). Neural data are extracted through tools such as electroencephalography, magnetic resonance imaging, magnetoencephalography, electrocorticography, and brain–computer interfaces. Each of these tools provides a specific type of information; for example, electroencephalography records surface electrical activity of the brain, whereas magnetic resonance imaging measures changes in cerebral blood flow associated with neuronal activity. These tools were initially developed for medical and research purposes, but they are now also used in commercial, military, educational, and even entertainment domains. This expansion of applications has exposed neural data to new threats. One important characteristic of neural data is that, unlike digital data, they cannot be changed or replaced. If a password or a person's digital information is disclosed, the individual can change it; however, if neural data are disclosed, they cannot be changed, because these data are connected to the individual's biological and cognitive structures. This characteristic makes neural data particularly vulnerable and increases the need for legal and criminal-law protection.

On the other hand, neural data may reveal information of which even the individual is unaware. Accordingly, neural patterns can disclose motor intentions, unconscious preferences, hidden emotional states, and even certain cognitive disorders before their behavioral manifestation. This degree of cognitive transparency has turned neural data into a powerful tool for analyzing the human mind; at the same time, however, it has increased the risk of their misuse.

Neural data have a set of unique characteristics that distinguish them from other types of data. The first characteristic is their direct reflection of mental states. Unlike biological data, which provide bodily information, or digital data, which indicate online behaviors, neural data are directly related to cognitive and emotional processes. These data can reveal an individual's emotions, intentions, preferences, and even thoughts. This very characteristic makes neural data the most sensitive type of data. If neural data are disclosed, the individual cannot change or replace them. Unlike passwords or digital information, these data are connected to the individual's biological and cognitive structures and cannot be altered. This characteristic makes neural data particularly vulnerable and increases the need for legal protection. Neural data constitute part of an individual's "mental identity" and can represent personal, cognitive, and emotional patterns. These data may show how an individual thinks, how they make decisions, and what emotions they experience. This level of cognitive transparency has made neural data a powerful tool for analyzing the human mind. Unauthorized access to neural data may lead to cognitive manipulation, the imposition of emotions, alteration of decision-making, or violation of mental privacy. This level of intervention is unprecedented in the history of criminal law, and traditional frameworks are unable to explain it. Therefore, neural data require special criminal-law protection.

2.2. The Difference Between Neural Data and Biological and Digital Data

Biological data such as DNA provide bodily information, and digital data indicate online behaviors; neural data, however, can reveal mental and cognitive structures. This difference fundamentally distinguishes neural data from other types of data. For example, electroencephalographic data can show patterns of attention, emotion, and even motor intention, whereas digital data merely record observable behaviors (Yuste, 2021). Another difference is that biological and digital data are usually changeable or replaceable, whereas neural data are not. If an individual's DNA is disclosed, its consequences are limited; however, if that person's neural data are disclosed, the consequences may include cognitive manipulation, the imposition of emotions, or the alteration of decision-making. This degree of harm is not observed in any other type of data. Neural data may also reveal information of which even the individual is unaware. This characteristic turns neural data into a powerful tool for analyzing the human mind, while also increasing the risk of their misuse. For example, studies have shown that neural patterns can reveal unconscious intentions before their behavioral manifestation. Ultimately, unlike digital data, neural data reveal not only observable behaviors but also hidden cognitive processes. This characteristic makes neural data the most sensitive type of data and increases the need for their legal and criminal-law protection.

3. Neurotechnologies and Contexts for the Commission of Crime

Neurotechnologies refer to a set of tools and systems based on neuroscience and neural engineering that make it possible to monitor, analyze, and intervene in human neural processes. Alongside their therapeutic and research functions, the expansion of these technologies has created new contexts for the commission of crimes and has introduced novel challenges in the fields of security and criminal law.

3.1. Brain–Computer Interfaces

Brain–computer interfaces are among the most important achievements of neuroscience and neural engineering in recent decades. These technologies enable direct communication between the human brain and digital systems and can receive and decode neural signals and convert them into machine-readable commands. Initially, brain–computer interfaces were developed to assist patients with paralysis or motor disorders; however, with technological progress, their applications have expanded into broader fields such as computer games, education, military uses, neuromarketing, and even the control of smart devices (Müller-Putz, 2020). This expansion of applications has transformed brain–computer interfaces from medical tools into general-purpose technologies with millions of potential users.

Despite their broad advantages, brain–computer interfaces have serious vulnerabilities. These devices are usually connected to processing systems through wireless waves or digital connections, which makes them vulnerable to intrusion, manipulation, or the interception of neural signals. Studies have shown that even non-invasive brain–computer interfaces such as electroencephalographic systems can provide sensitive information about an individual's cognitive and emotional states (Choi & Kim, 2022). If accessed without authorization, this information may be used for personality analysis, behavioral prediction, or even cognitive manipulation.

One of the major challenges of brain–computer interfaces is the absence of unified security standards. Many commercial brain–computer interface devices are designed for ease of use rather than security. These devices often lack strong encryption, multi-factor authentication, or advanced security protocols. These weaknesses make it possible to penetrate the device and access neural data. Some studies have shown that even simple machine learning algorithms can extract information from electroencephalographic signals about a user's preferences or emotional reactions (Goering & Yuste, 2021). This level of vulnerability has turned brain–computer interfaces into one of the most important contexts for the commission of neurocybercrimes. Ultimately, it must be noted that brain–computer interfaces are not merely tools for extracting neural data; they can also be used for reverse brain stimulation. This capability makes it possible to send signals to the brain and influence an individual's cognitive or emotional states. This degree of intervention is unprecedented in the history of technology and may produce profound and irreversible consequences (Müller-Putz, 2020). Therefore, brain–computer interfaces are not only rehabilitation tools but also potential instruments for cognitive control and the commission of neurocybercrimes.

3.2. The Role of Artificial Intelligence in the Analysis of Neural Data

Artificial intelligence, especially deep learning algorithms, plays a decisive role in the analysis of neural data. Neural data are usually complex, large-scale, and highly noisy, and their analysis using traditional methods is difficult. Deep learning algorithms, however, can identify hidden patterns in neural data and extract information about an individual's cognitive states, emotions, intentions, and even decision-making processes (Rashid, 2020). This capability has made mind decoding possible and has created new threats. One of the major challenges of artificial intelligence in the analysis of neural data is the opacity of algorithms. Many deep learning models, such as convolutional or recurrent neural networks, have complex structures and their decision-making processes cannot be explained. This feature turns neural-data analysis into a "black box" in which it is unclear how the algorithm has reached its conclusion (Goering & Yuste, 2021). This level of ambiguity increases the risk of misuse of neural data, because algorithms may extract information of which even the user is unaware.

Another challenge is the ability of artificial intelligence to predict behavior. Machine learning algorithms can use neural data to predict an individual's behavioral patterns and even anticipate their reactions in different situations. This capability has applications in fields such as neuromarketing or targeted advertising; at the same time, however, it can also be used for cognitive manipulation or behavioral control (Zuboff, 2019). This level of intervention is unprecedented in the history of technology and requires new legal and ethical frameworks. Ultimately, it must be noted that artificial intelligence is not only a tool for analyzing neural data but can also be used to generate synthetic neural data. These data may be used to train models, simulate cognitive states, or even deceive security systems (Rashid, 2020). This level of complexity has turned neural-data analysis into one of the most challenging areas of technology.

4. Cognitive Victimization

Cognitive victimization is an emerging concept in criminology and criminal law that refers to harms that directly target an individual's mental processes, cognitive states, decision-making structures, and mental privacy. Unlike traditional victimization, which focuses on physical or financial harm, cognitive victimization emphasizes a level of harm in which the "mind" becomes the object of crime. This type of victimization has emerged as a result of the development of neurotechnologies and the possibility of extracting or manipulating neural data. Neural data can reveal information about an individual's intentions, emotions, and preferences, thereby turning the human mind into a potential target for abuse (Ienca, 2023).

Cognitive victimization occurs when an individual, without awareness or consent, is exposed to intervention in their cognitive processes. This intervention may include the unauthorized extraction of neural data, manipulation of emotions, imposition of thoughts, or alteration of decision-making patterns. In this type of victimization, harms are not necessarily visible, and the individual may not even become aware of their occurrence. This feature distinguishes cognitive victimization from other types of victimization and makes it one of the most complex challenges of contemporary criminal law (Yuste & Goering, 2022). One of the important characteristics of cognitive victimization is its immaterial and hidden nature. Unlike physical harms, which are visible and measurable, cognitive harms may occur only at the mental level and have no external sign. For example, cognitive manipulation may appear as subtle changes in preferences, emotions, or decision-making without the individual becoming aware of its cause. This level of concealment makes cognitive victimization one of the most challenging domains of criminology (Lavazza & Massimini, 2023). Ultimately, cognitive victimization harms not only the individual's privacy but also their "mental integrity." Mental integrity refers to the individual's right to preserve their cognitive and emotional structures against unauthorized intervention. Violation of this right has existential and identity-related consequences and may lead to long-term changes in personality, behavior, or emotions. Therefore, cognitive victimization requires new legal and ethical frameworks capable of protecting the human mind against emerging threats (Ienca & Andorno, 2024).

4.1. Definition of the Cognitive Victim

Cognitive victimization has various dimensions, each representing a specific type of harm. The first dimension is harm to mental autonomy. Mental autonomy refers to the individual's ability to control their own thoughts, emotions, and decisions. When neurotechnologies or artificial intelligence algorithms influence an individual's cognitive processes without consent,

their mental autonomy is violated. This type of harm may lead to unwanted changes in behavior, preferences, or decision-making (Bublitz, 2022).

The second dimension is cognitive distortion. Cognitive distortion occurs when an individual's neural data are manipulated or false information is sent to their brain. This type of intervention may lead to changes in perception, memory, or emotions. For example, non-invasive brain stimulation can strengthen or weaken positive or negative emotions, and this may occur without the individual's awareness (Kadosh, 2021).

The third dimension is emotional manipulation. Neural data can provide precise information about an individual's emotional states, thereby making it possible to manipulate emotions. For example, artificial intelligence algorithms can use neural patterns to predict an individual's emotional reactions and then use this information to influence their emotions. This type of manipulation may have broad psychological and social consequences (Reardon, 2023). The fourth dimension is the violation of cognitive privacy. Cognitive privacy refers to the individual's right to preserve their thoughts, emotions, and intentions against unauthorized access. Neural data can violate this privacy and reveal information of which even the individual is unaware. This level of cognitive transparency increases the risk of misuse of neural data and highlights the need for legal protection of cognitive privacy (Ienca, 2023).

4.2. The Difference Between Cognitive Victimization and Psychological Victimization

Cognitive victimization and psychological victimization are two different concepts, although they may overlap in some cases. Psychological victimization usually refers to harms that arise as a result of traumatic experiences and include anxiety, depression, fear, or psychological disorders. These harms are usually the consequence of an external event, and the individual is aware of their occurrence (Herman, 2022). By contrast, cognitive victimization directly targets an individual's mental and cognitive structures and may occur without their awareness. This type of victimization may include emotional manipulation, imposition of thoughts, or alteration of decision-making patterns. Unlike psychological victimization, which is the consequence of an event, cognitive victimization is the cause of harm and may lead to long-term changes in personality or behavior (Lavazza & Massimini, 2023). Another difference between these two concepts lies in the nature of the harms. Psychological harms are usually observable or diagnosable and can be measured using psychological instruments. Cognitive harms, however, may occur at the mental level and have no external sign. This feature makes cognitive victimization one of the most complex areas of criminology (Ienca, 2023). Ultimately, because of its direct connection with neural data and emerging technologies, cognitive victimization requires new legal and ethical frameworks. This type of victimization harms not only the individual's mental health but also their "mental integrity," a concept that has no established place in traditional criminal law (Yuste & Goering, 2022).

5. Neurocybercrimes

Neurocybercrimes refer to a set of criminal behaviors that directly target neural data, neural–digital systems, or human cognitive processes. These crimes have emerged as a result of the integration of neurotechnologies with artificial intelligence and digital networks, and they have a nature completely different from traditional cybercrimes. In neurocybercrimes, the object of the crime is not digital data but the human "mind" and "cognition." Recent studies show that these crimes may include neural-data theft, cognitive manipulation, mind decoding, cognitive surveillance, and cognitive imposition (Ienca, 2023).

One of the most important types of neurocybercrimes is neural-data theft. In this type of crime, the attacker penetrates brain–computer interface devices or neural-data storage systems and extracts information about an individual's mental states, emotions, preferences, or intentions. Unlike digital-data theft, this type of theft may have existential consequences, because neural data constitute part of an individual's cognitive identity and their disclosure may lead to extensive misuse (Yuste & Goering, 2022).

Another type of neurocybercrime is cognitive manipulation. In this type of crime, the attacker influences an individual's emotions, thoughts, or decision-making through non-invasive brain stimulation, artificial intelligence algorithms, or the manipulation of neural data. This type of intervention may occur without the individual's awareness and may have long-term

consequences for their behavior or personality. Studies have shown that brain stimulation can strengthen or weaken positive or negative emotions, and this can be used for criminal purposes (Kadosh, 2021). Ultimately, mind decoding and cognitive surveillance are also among the most important types of neurocybercrimes. In mind decoding, the attacker attempts to extract an individual's thoughts or intentions through the analysis of neural data. In cognitive surveillance, the attacker continuously monitors the individual's cognitive states. These types of crimes violate the individual's cognitive privacy and may have broad psychological and social consequences (Reardon, 2023).

5.1. Consequences of Neurocybercrime

Neurocybercrimes have profound and multilayered consequences that affect not only an individual's mental health but also their cognitive identity and mental integrity. The first consequence is the loss of mental control. When an individual's neural data are extracted or manipulated, they may lose control over their thoughts, emotions, or decision-making. This type of harm has an existential nature and may lead to long-term changes in personality or behavior (Ienca & Andorno, 2024).

The second consequence is harm to cognitive identity. Neural data constitute part of an individual's mental identity, and intrusion into them may result in the distortion or alteration of that identity. For example, cognitive manipulation may change an individual's preferences, beliefs, or emotions, which can have broad social and psychological consequences (Lavazza & Massimini, 2023).

The third consequence is unwanted changes in decision-making. Brain stimulation or manipulation of neural data can affect decision-making processes and push an individual toward decisions that are inconsistent with their actual values or preferences. This type of intervention violates the individual's mental autonomy and may have broad legal and ethical consequences (Bublitz, 2022). Ultimately, neurocybercrimes may lead to the violation of mental integrity. Mental integrity refers to the individual's right to preserve their cognitive and emotional structures against unauthorized intervention. Violation of this right has existential consequences and may lead to long-term changes in personality, behavior, or emotions. This level of harm is not observed in any other type of crime and requires new legal frameworks (Yuste & Goering, 2022).

5.2. Types of Neurocybercrimes

Neurocybercrimes encompass a spectrum of criminal behaviors that directly target an individual's neural data, cognitive structures, or mental processes. The first type of these crimes is neural-data theft. In this type of crime, the attacker penetrates brain–computer interface devices, neural implants, or neural-data storage systems and extracts information about an individual's mental states, emotions, preferences, or intentions. Unlike digital-data theft, this type of theft has existential consequences, because neural data constitute part of the individual's cognitive identity and their disclosure may lead to extensive misuse (Ienca, 2023).

The second type is the manipulation of neural data. In this type of crime, the attacker alters an individual's neural data or sends false information to their brain. This intervention may lead to the distortion of emotions, alteration of preferences, or disruption of decision-making. Studies have shown that non-invasive brain stimulation can strengthen or weaken positive or negative emotions, and this can be used for criminal purposes (Kadosh, 2021).

The third type is mind decoding. In this type of crime, the attacker attempts to extract an individual's thoughts, intentions, or emotions through the analysis of neural data. Deep learning algorithms can identify hidden patterns in electroencephalographic or magnetic resonance imaging data and provide information about the individual's cognitive states. This level of cognitive transparency increases the risk of misuse of neural data (Reardon, 2023).

The fourth type is cognitive imposition. In this type of crime, the attacker attempts to impose specific thoughts, emotions, or decisions on the individual. This type of intervention may be carried out through brain stimulation, artificial intelligence algorithms, or manipulation of neural data. This level of intervention is unprecedented in the history of technology and has existential consequences (Lavazza & Massimini, 2023). Therefore, unlike traditional cybercrimes, these crimes do not merely harm data or infrastructure but directly target the "mind." This transformation has important theoretical implications for criminology. Criminology must expand from the behavioral and social levels of analysis to the cognitive and neural levels. In

neurocybercrimes, criminal behavior occurs not only in digital space but also in "mental space," a space that has not previously been the object of criminological analysis. These crimes show that the concept of "harm" in criminal law must be redefined. In traditional crimes, harm is usually visible and measurable; in neurocybercrimes, however, harms occur at the mental level and may have no external sign. This feature reveals the need to develop new tools for detecting, proving, and measuring cognitive harms.

Neurocybercrimes show that the boundary between "victim" and "offender" may become more ambiguous in the future. For example, if an algorithm influences an individual's decision-making without their awareness, is that individual responsible for their behavior? This question has important implications for criminal responsibility and shows that criminal law must seriously address the issue of "cognitive autonomy."

Ultimately, the analysis of the types of neurocybercrimes shows that these crimes are not only a threat to individual security but also a threat to "cognitive liberty" and "mental integrity." This level of threat highlights the need to develop cognitive rights and new criminalizations.

6. Consequences of Victimization in Neurocybercrimes

The consequences of victimization in neurocybercrimes are multilayered and complex. Neural data can provide information about an individual's emotions, intentions, and preferences, and intrusion into them can violate the individual's mental privacy. This type of harm has broad psychological and social consequences and may lead to anxiety, distrust, or a sense of cognitive insecurity (Ienca, 2023). When an individual's neural data are manipulated or false information is sent to their brain, they may lose control over their thoughts, emotions, or decision-making. This type of harm has an existential nature and may lead to long-term changes in personality or behavior (Bublitz, 2022). Mental integrity refers to the individual's right to preserve their cognitive and emotional structures against unauthorized intervention. Violation of this right has existential consequences and may lead to long-term changes in personality, behavior, or emotions (Ienca & Andorno, 2024). In this regard, neural data constitute part of an individual's cognitive identity, and intrusion into them may lead to the distortion or alteration of this identity. This type of harm has broad social and psychological consequences and may lead to an identity crisis or cognitive disorders (Lavazza & Massimini, 2023).

Therefore, these crimes do not merely harm data or privacy; they damage the individual's "cognitive identity" and "mental integrity." This level of harm is not observed in any other type of crime and requires new theoretical frameworks. Cognitive victimization shows that the concept of "harm" must be expanded from the physical and financial levels to the cognitive and existential levels. This transformation has important implications for criminal law and shows that existing laws are unable to protect victims of neurocybercrime. The human mind must be recognized as a "protected domain" in criminal law. This domain includes not only thoughts and emotions but also decision-making processes and cognitive structures. Intrusion into this domain must be recognized as an independent crime, and proportionate punishments must be prescribed for it. Victims of neurocybercrime require special protections. These protections must include psychological, legal, and social support. For example, victims may need cognitive assessments, psychological treatments, or legal assistance in order to manage the consequences of victimization. Ultimately, the analysis of the consequences of cognitive victimization shows that neurocybercrimes are not only a threat to individual security but also a threat to "cognitive liberty" and "human dignity." This level of threat highlights the need to develop cognitive rights and new criminalizations.

7. Criminal-Law Challenges in Confronting Neurocybercrimes

One of the most important challenges of criminal law in confronting neurocybercrimes is the absence of a clear legal definition of neural data. In many legal systems, data are divided into two general categories: "personal data" and "sensitive data"; however, neural data do not fit precisely into either of these categories. Neural data are not only personal information but also information about an individual's mental states, emotions, and cognitive processes. This level of sensitivity reveals the need for a new legal definition of neural data (Ienca & Andorno, 2024).

The second challenge is the difficulty of proving the crime. Neurocybercrimes usually occur without external signs, and the victim may not even become aware that a crime has occurred. For example, cognitive manipulation or extraction of neural data

may take place without any physical effect. This characteristic makes proof of the crime difficult and requires the development of new tools for detecting and documenting cognitive harms (Reardon, 2023). The third challenge is criminal responsibility in situations of cognitive manipulation. If an individual makes a decision or engages in behavior under the influence of cognitive manipulation, can they be held responsible? This question has important implications for criminal law and shows that the concept of "free will" must be redefined in light of neurotechnologies. Recent studies show that brain stimulation can influence decision-making, and this may affect criminal responsibility (Kadosh, 2021).

The fourth challenge is the absence of specific criminalizations. Many legal systems lack regulations that specifically address neurocybercrimes. This legal gap increases the possibility of misuse of neurotechnologies and leaves victims without criminal-law protection. Therefore, the development of new laws for the protection of mental integrity and cognitive privacy is necessary (Lavazza & Massimini, 2023). Accordingly, existing legal systems were not designed to confront neurocybercrimes. First, traditional criminal law has been formed on the basis of "visible harms"; however, neurocybercrimes create harms that occur at the mental level and may have no external sign. This feature reveals the need to develop new tools for detecting and proving cognitive harms. Second, neurocybercrimes show that the concept of "criminal responsibility" must be redefined. If an individual makes a decision under the influence of cognitive manipulation, they cannot be considered fully responsible. This issue has important implications for criminal law and shows that a distinction must be made between "free will" and "manipulated will."

Third, the analysis of criminal-law challenges shows that the human mind must be recognized as a "protected domain" in criminal law. This domain includes thoughts, emotions, intentions, and cognitive processes. Intrusion into this domain must be recognized as an independent crime, and proportionate punishments must be prescribed for it.

Ultimately, criminal-law challenges show that the development of "cognitive rights" and "new criminalizations" is necessary. These rights must include the right to mental integrity, the right to cognitive privacy, the right to mental autonomy, and the right not to be subjected to cognitive manipulation.

8. The Need to Redefine Victimization in Light of Neurocybercrimes

The emergence of neurocybercrimes shows that the concept of victimization must be redefined. In traditional victimization, harms are usually physical, financial, or reputational; however, in cognitive victimization, harms occur at the mental level and may have no external sign. This feature reveals the need to develop new theoretical frameworks (Ienca, 2023). One of the most important reasons for redefining victimization is the cognitive nature of harms. Neural data can provide information about an individual's emotions, intentions, and cognitive processes, and intrusion into them may lead to cognitive manipulation or the imposition of emotions. This level of harm is not observed in any other type of crime and requires new theoretical frameworks (Bublitz, 2022). Another reason is the connection between neural data and cognitive identity. Neural data constitute part of an individual's mental identity, and intrusion into them may lead to the distortion or alteration of this identity. This type of harm has existential consequences and may lead to an identity crisis or cognitive disorders (Lavazza & Massimini, 2023). Ultimately, redefining victimization is necessary because neurocybercrimes can occur without the individual's awareness. This feature distinguishes cognitive victimization from traditional victimization and shows that a distinction must be made between "visible harms" and "hidden cognitive harms" (Reardon, 2023). Criminology must expand from the behavioral and social levels of analysis to the cognitive level. In neurocybercrimes, the victim may have no external sign of harm but may have suffered deep injuries at the mental level. This feature reveals the need to develop new tools for detecting and measuring cognitive harms. Second, redefining victimization shows that the human mind must be recognized as a "protected domain" in criminology. This domain includes thoughts, emotions, intentions, and cognitive processes. Intrusion into this domain must be recognized as a new type of victimization. Third, redefining victimization shows that victims of neurocybercrime require special protections. These protections must include psychological, legal, and social support. For example, victims may need cognitive assessments, psychological treatments, or legal assistance in order to manage the consequences of victimization.

9. The Role of Cognitive Rights in Protecting Victims of Neurocybercrime

Cognitive rights are a set of emerging rights designed to protect the human mind against neurotechnologies. These rights include the right to mental integrity, the right to cognitive privacy, the right to mental autonomy, and the right not to be subjected to cognitive manipulation. These rights are a response to the emerging threats of neurotechnologies and can protect victims of neurocybercrime (Ienca & Andorno, 2024). One of the most important cognitive rights is the right to mental integrity. This right allows the individual to preserve their cognitive and emotional structures against unauthorized intervention. Violation of this right has existential consequences and may lead to long-term changes in personality or behavior (Yuste & Goering, 2022). Another right is the right to cognitive privacy. This right allows the individual to preserve their thoughts, emotions, and intentions against unauthorized access. Neural data can violate this privacy and reveal information of which even the individual is unaware (Reardon, 2023). Ultimately, cognitive rights can provide a framework for new criminalizations. These rights can serve as a basis for developing new laws that protect the human mind against emerging threats (Lavazza & Massimini, 2023). These rights can fill existing gaps in criminal law. First, cognitive rights can serve as a basis for new criminalizations. For example, intrusion into mental integrity or cognitive privacy can be recognized as an independent crime. Second, cognitive rights can protect victims of neurocybercrime. These protections may include legal, psychological, and social support. For example, victims may need cognitive assessments or psychological treatments. Third, cognitive rights can provide a framework for the development of public policies. These policies may include regulations for the protection of neural data, security standards for brain–computer interface devices, and restrictions on the use of neurotechnologies. These crimes directly target an individual's neural data, cognitive processes, and mental structures and have existential consequences. This level of harm is not observed in any other type of crime and requires new theoretical frameworks (Ienca, 2023). Therefore, cognitive victimization has a nature different from traditional victimization. This type of victimization occurs at the mental level and may have no external sign. This feature reveals the need to develop new tools for detecting and measuring cognitive harms (Bublitz, 2022). Ultimately, the third chapter showed that existing criminal law is unable to protect victims of neurocybercrime. This legal gap highlights the need to develop cognitive rights and new criminalizations (Lavazza & Massimini, 2023). Therefore, neurocybercrimes are not only a threat to individual security but also a threat to "cognitive liberty" and "human dignity." This level of threat highlights the need to develop cognitive rights and new criminalizations. The human mind must be recognized as a "protected domain" in criminal law. This domain includes thoughts, emotions, intentions, and cognitive processes. Intrusion into this domain must be recognized as an independent crime. Ultimately, victims of neurocybercrime require special protections. These protections must include psychological, legal, and social support.

10. Legal, Policy, and Criminalization Strategies for Confronting Neurocybercrimes

Rapid developments in neurotechnology and its integration with artificial intelligence have created unprecedented challenges for legal systems. As shown in the third chapter, neurocybercrimes have a complex, multilayered, and hidden nature and can lead to cognitive, existential, and identity-related harms. This level of harm cannot be explained within any of the traditional criminal-law frameworks and requires a fundamental reconsideration of laws, policies, and protective mechanisms (Ienca & Andorno, 2024). One of the most important necessities in this field is the creation of new legal frameworks for the protection of neural data. Neural data are not merely personal information; they also provide information about an individual's mental states, emotions, and cognitive processes. This level of sensitivity reveals the need to create specific laws for the protection of neural data (Yuste & Goering, 2022). Existing laws on personal data are unable to protect neural data, because these data have a cognitive nature and can be used for mental manipulation. On the other hand, neurocybercrimes show that cognitive rights must be recognized as an independent field within human rights and criminal law. These rights include the right to mental integrity, the right to cognitive privacy, the right to mental autonomy, and the right not to be subjected to cognitive manipulation. These rights can serve as a basis for new criminalizations and for the protection of victims of neurocybercrime (Lavazza & Massimini, 2023). Ultimately, by presenting legal and criminalization strategies, a comprehensive framework for confronting neurocybercrimes can be provided. These strategies not only help protect victims but can also prevent the occurrence of crimes. Existing legal systems were not designed to confront neurocybercrimes. Existing

laws on personal data are unable to protect neural data, because neural data have a cognitive nature and can be used for mental manipulation. This feature reveals the need to create specific laws for the protection of neural data. Cognitive rights must be recognized as an independent field within human rights and criminal law. These rights can serve as a basis for new criminalizations and for the protection of victims of neurocybercrime. For example, intrusion into mental integrity or cognitive privacy can be recognized as an independent crime. Policy in the field of neurotechnology must be based on ethical and legal principles. These policies must include regulations for the protection of neural data, security standards for brain–computer interface devices, and restrictions on the use of neurotechnologies.

11. The Need for Specific Criminalization of Neurocybercrimes

One of the most important necessities in confronting neurocybercrimes is the creation of specific criminalizations. Existing criminal laws have largely been designed for traditional crimes and are unable to explain cognitive harms. For example, laws on data theft cover only digital data and do not include neural data. This legal gap increases the possibility of misuse of neurotechnologies and leaves victims without criminal-law protection (Ienca, 2023). Specific criminalization must include behaviors such as neural-data theft, cognitive manipulation, mind decoding, cognitive surveillance, and cognitive imposition. These behaviors have a cognitive nature and may lead to existential harms. Therefore, they must be recognized as independent crimes, and proportionate punishments must be determined for them (Bublitz, 2022). One of the most important challenges in specific criminalization is the precise definition of cognitive concepts. For example, it must be clarified exactly what "mental integrity" or "cognitive privacy" means and what behaviors violate them. These definitions must be based on neuroscience, cognitive psychology, and technology ethics (Lavazza & Massimini, 2023). Ultimately, specific criminalization must be consistent with international standards. Neurocybercrimes are usually transnational, and the victim may be in one country while the offender operates in another. This feature reveals the need for international cooperation (Yuste & Goering, 2022). Neurocybercrimes have a nature completely different from traditional crimes and cannot be explained through existing laws. These crimes create harms that occur at the mental level and may have no external sign. This feature reveals the need to create new criminalizations. Specific criminalization must be based on neuroscience and cognitive psychology. These sciences can help define concepts such as "mental integrity" or "cognitive privacy" with precision. These definitions must form the basis for new criminalizations. Third, specific criminalization must be harmonized with international standards. Neurocybercrimes are usually transnational and require international cooperation. Such cooperation may include information exchange, legal harmonization, and the creation of joint mechanisms for confronting neurocybercrimes.

12. Developing a Framework of Cognitive Rights in the Criminal-Law System

Developing a framework of cognitive rights in the criminal-law system is one of the most important steps for confronting neurocybercrimes. Cognitive rights are a set of emerging rights designed to protect the human mind against neurotechnologies. These rights include the right to mental integrity, the right to cognitive privacy, the right to mental autonomy, and the right not to be subjected to cognitive manipulation. These rights can serve as a basis for new criminalizations and for the protection of victims of neurocybercrime (Ienca & Andorno, 2024). One of the most important elements of the cognitive-rights framework is the right to mental integrity. This right allows the individual to preserve their cognitive and emotional structures against unauthorized intervention. Violation of this right has existential consequences and may lead to long-term changes in the individual's personality or behavior. This level of harm is not observed in any other type of crime and requires independent criminalization (Yuste & Goering, 2022). Another element is the right to cognitive privacy. This right allows the individual to preserve their thoughts, emotions, and intentions against unauthorized access. Neural data can violate this privacy and reveal information of which even the individual is unaware. This feature reveals the need to create specific laws for the protection of neural data (Reardon, 2023). Ultimately, the cognitive-rights framework must include the right to mental autonomy. This right allows the individual to control their thoughts, emotions, and decisions without external intervention. Cognitive manipulation or the imposition of emotions violates this right and may have broad psychological and social consequences (Lavazza & Massimini, 2023). These rights can fill existing gaps in criminal law. First, cognitive rights can serve as a basis for new

criminalizations. For example, intrusion into mental integrity or cognitive privacy can be recognized as an independent crime. These criminalizations must be based on neuroscience and cognitive psychology so that they can precisely explain cognitive harms. Second, cognitive rights can protect victims of neurocybercrime. These protections may include legal, psychological, and social support. For example, victims may need cognitive assessments or psychological treatments in order to manage the consequences of victimization. Third, cognitive rights can provide a framework for developing public policies. These policies may include regulations for the protection of neural data, security standards for brain–computer interface devices, and restrictions on the use of neurotechnologies.

13. Creating Security Standards for Neurotechnologies

One of the most important strategies for confronting neurocybercrimes is the creation of security standards for neurotechnologies. Many brain–computer interface devices or neuroimaging tools lack appropriate security standards, which makes them vulnerable to intrusion, manipulation, or interception of neural signals (Choi & Kim, 2022). These vulnerabilities can lead to neural-data theft or cognitive manipulation. Security standards must include strong encryption of neural data, multi-factor authentication, and advanced security protocols. These standards can prevent intrusion into brain–computer interface devices and increase the security of neural data. Studies show that encryption of neural data can significantly reduce the risk of intrusion (Müller-Putz, 2020). Neural data are usually stored on cloud servers, and this exposes them to risk. Therefore, regulations must be established to protect neural data during storage and transmission (Goering & Yuste, 2021). Ultimately, security standards must include regulations for the design of brain–computer interface devices. These regulations must include security requirements for hardware, software, and artificial intelligence algorithms. These standards can prevent the misuse of neurotechnologies (Rashid, 2020). The security of neurotechnologies must be designed at three levels: hardware, software, and data. At the hardware level, brain–computer interface devices must have built-in security systems that prevent intrusion. At the software level, artificial intelligence algorithms must have security protocols that prevent data manipulation. At the data level, neural data must be encrypted in order to prevent their disclosure. Second, the analysis of security standards shows that the security of neurotechnologies must be based on ethical principles. These principles must include respect for cognitive privacy, mental integrity, and mental autonomy. These principles can serve as the basis for developing security standards. Third, the analysis of security standards shows that international cooperation is necessary. Neurotechnologies are usually transnational and require international cooperation for the development of security standards.

14. Developing Support Mechanisms for Victims of Neurocybercrime

One of the most important strategies for confronting neurocybercrimes is the development of support mechanisms for victims. Victims of neurocybercrime usually suffer cognitive, psychological, and existential harms and require special support. These protections must include legal, psychological, and social support (Herman, 2022). Legal support must include access to lawyers specialized in neurotechnologies, judicial support, and compensation for cognitive harm. These forms of support can help victims manage the consequences of victimization (Ienca, 2023). Psychological support must include cognitive assessments, psychological treatments, and specialized counseling. These forms of support can help victims manage cognitive harms (Lavazza & Massimini, 2023). Ultimately, social support must include public education about neurocybercrimes, the establishment of support centers, and cognitive rehabilitation programs. These forms of support can help victims return to normal life (Reardon, 2023). Victims of neurocybercrime require multilayered support. First, legal support must include compensation for cognitive harm. This type of harm has a cognitive nature and must be compensated independently. Second, psychological support must be based on neuroscience and cognitive psychology. These supports must include cognitive assessments and psychological treatments. Third, social support must include public education about neurocybercrimes. Such education can help increase public awareness and prevent the occurrence of crimes.

15. Conclusion

Extensive developments in neurotechnology and its integration with artificial intelligence have transformed the traditional boundaries between humans and machines and have paved the way for the emergence of a new category of crimes that directly target the human mind, cognition, and neural data. These crimes, analyzed in this study under the title "neurocybercrimes," have a multilayered, hidden, and complex nature and can lead to harms that are not merely physical or financial but directly affect the individual's cognitive and identity structures. This level of harm cannot be explained within any of the traditional frameworks of criminal law, and this reveals the need for a fundamental reconsideration of the foundational concepts of criminal law. Neural data have a nature completely different from digital or biological data. These data are direct reflections of an individual's mental states, emotions, intentions, and cognitive processes, and for this reason their sensitivity and vulnerability are much greater than those of other types of data. Intrusion into neural data is not only a violation of privacy but also an intrusion into the individual's "mental integrity" and "cognitive identity." This characteristic highlights the need to create specific laws for the protection of neural data.

This type of victimization occurs at the mental level and may have no external sign. The victim may not even become aware that the crime has occurred but may suffer deep and long-term harms at the cognitive level. This feature reveals the need to develop new tools for detecting, proving, and measuring cognitive harms.

Ultimately, existing criminal law is unable to protect victims of neurocybercrime. This legal gap highlights the need to develop "cognitive rights" and "new criminalizations." Cognitive rights can serve as a basis for protecting the human mind against the emerging threats of neurotechnologies and can provide a framework for the development of new laws. The conclusion of the study shows that neurocybercrimes are not merely a technological threat but also a philosophical, ethical, and legal threat. These crimes challenge the traditional concept of "harm" and show that harm can occur at the mental level without any external sign. This transformation has important implications for criminal law and shows that a distinction must be made between "visible harms" and "hidden cognitive harms." On the other hand, the human mind must be recognized as a "protected domain" in criminal law. This domain includes thoughts, emotions, intentions, and cognitive processes. Intrusion into this domain must be recognized as an independent crime, and proportionate punishments must be determined for it. Victims of neurocybercrime require special protections. These protections must include psychological, legal, and social support. For example, victims may need cognitive assessments or psychological treatments in order to manage the consequences of victimization.

15.1. Recommendations

1. Creating Specific Laws for Neural Data

The legislature must recognize neural data as an independent category of data and develop special regulations for their collection, storage, processing, and transfer. These laws must take into account the cognitive sensitivity of neural data and prescribe proportionate punishments for their misuse.

2. Independent Criminalization of Neurocybercrimes

Behaviors such as neural-data theft, cognitive manipulation, mind decoding, cognitive surveillance, and cognitive imposition must be recognized as independent crimes. These criminalizations must be based on the cognitive nature of harms, not on traditional criteria of physical or financial harm.

3. Establishing Specialized Institutions for Addressing Neurocybercrimes

Addressing these crimes requires expertise in neuroscience, cognitive psychology, cybersecurity, and criminal law. The establishment of specialized prosecution offices or committees can help detect and prove these crimes.

4. Developing Cognitive Rights in the Legal System

Rights such as the right to mental integrity, the right to cognitive privacy, and the right to mental autonomy must be recognized as fundamental human rights in domestic law.

5. Creating Security Standards for Neurotechnologies

Brain–computer interface devices and other neurotechnologies must have strict security standards. These standards must include encryption of neural data, multi-factor authentication, and advanced security protocols.

6. Public Education About the Risks of Neurocybercrimes

Many users are unaware of the risks of these technologies. Public education can help increase awareness and reduce victimization.

7. Establishing Support Centers for Victims of Neurocybercrime

These centers must include psychological, legal, and social services and help victims manage the consequences of victimization.

8. Establishing International Cooperation

Neurocybercrimes are usually transnational and require international cooperation to confront them.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Bublitz, J. C. (2022). *Cognitive Liberty and Mental Autonomy in the Age of Neurotechnology*. Oxford University Press.
Choi, J., & Kim, S. (2022). Security Vulnerabilities in Consumer-Grade Brain-Computer Interfaces. *Neurocomputing*, *512*, 145-158.
Farahany, N. (2023). *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology*. St. Martin's Press.
Goering, S., & Yuste, R. (2021). Ethical Challenges of Neurotechnology. *Nature Reviews Neuroscience*, *22*(10), 611-622.
Greely, H. (2021). *Neuroethics and the Law*. Oxford University Press.
Herman, J. (2022). *Trauma and Recovery: The Aftermath of Violence*. Basic Books.
Ienca, M. (2021). Neuroprivacy: Emerging Challenges. *Nature Biotechnology*, *39*(2), 147-150.
Ienca, M. (2023). *The Rise of Neurodata: Ethical and Legal Challenges*. MIT Press.
Ienca, M., & Andorno, R. (2017). Towards New Human Rights in the Age of Neuroscience and Neurotechnology. *Life Sciences, Society and Policy*, *13*(5), 1-27.
Ienca, M., & Andorno, R. (2024). *Neurorights and Mental Integrity*. Cambridge University Press.
Kadosh, R. C. (2021). Non-invasive Brain Stimulation and Cognitive Modulation. *Nature Reviews Neuroscience*, *22*(5), 298-310.
Lavazza, A., & Massimini, M. (2023). *The Ethics of Cognitive Enhancement and Mental Privacy*. Springer.
Müller-Putz, G. (2020). Brain-Computer Interfaces: Applications and Risks. *IEEE Transactions on Neural Systems*, *28*(4), 987-995.
Oecd. (2019). *Recommendation on Responsible Innovation in Neurotechnology*.
Rashid, M. (2020). Deep Learning for Neural Decoding. *Trends in Neurosciences*, *43*(11), 825-839.
Reardon, S. (2023). Emotion AI and the Future of Human Autonomy. *Science*, *381*(6652), 15-20.
Unesco. (2021). *Ethics of Neurotechnology Report*.
Yuste, R. (2017). Four Ethical Priorities for Neurotechnologies and AI. *Nature*, *551*, 159-163.
Yuste, R. (2021). Four Ethical Priorities for Neurotechnologies and AI. *Nature*, *551*(7679), 159-163.
Yuste, R., & Goering, S. (2022). Neurotechnology, Ethics, and Society. *Nature Neuroscience*, *25*(2), 110-118.
Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.