Научная статья
УДК 34:004:343.721:004.8
EDN: https://elibrary.ru/smgmxq
DOI: https://doi.org/10.21202/jdtl.2025.16

Нейрохакинг в эпоху цифровизации и искусственного интеллекта: правовые аспекты защиты нейронной информации

Диого Перейра Коэльо

Севильский университет, Севилья, Испания

Ключевые слова

интерфейс «мозг – компьютер»,
искусственный интеллект,
киберпреступность,
метавселенная,
нейробезопасность,
нейропреступность,
нейротехнологии,
нейрохакинг,
право,
цифровые технологии

Аннотация

Цель: внесение вклада в осмысление концепции нейропреступности, а также в изучение текущих и будущих рисков с точки зрения нейробезопасности в условиях развития цифровизации и искусственного интеллекта.

Методы: в исследовании применен критико-описательный анализ связи между киберпреступностью и нейропреступностью, проведено концептуальное разграничение интерфейса «мозг – компьютер» и вариантов его использования, выполнено описание различий между нейронными и психическими манипуляциями. Исследуется правовая автономия преступлений против психической неприкосновенности по отношению к преступлениям против физической неприкосновенности. Методологический аппарат включает анализ существующих прототипов нейропреступлений на основе четырехфазного цикла интерфейса «мозг – компьютер» и изучение специфики нейрохакинга в контексте метавселенной и технологий искусственного интеллекта.

Результаты: исследование выявило сущностные характеристики нейрохакинга как неправомерного использования нейронных устройств для получения несанкционированного доступа к нейронной информации и ее манипулирования. Определены четыре основных типа приложений интерфейса «мозг – компьютер», подверженных нейрохакингу: нейромедицинские приложения, системы аутентификации пользователей, видеоигры и приложения на базе смартфонов. Установлены модальности нейрохакинга на каждой фазе цикла интерфейса «мозг – компьютер»: манипуляции на этапе ввода нейронной информации, измерения и записи мозговой активности, декодирования и классификации нейронной информации, а также на этапе вывода результата. Проанализированы специфические угрозы нейрохакинга в эпоху цифровизации, включая иммерсивные атаки и атаки типа «человек – джойстик» в метавселенной.

© Коэльо Д. П., 2025

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Научная новизна: впервые проведено комплексное разграничение концепций нейропреступности и киберпреступности с выделением их специфических правовых последствий. Предложена авторская классификация нейропреступлений на основе четырехфазного цикла интерфейса «мозг – компьютер». Обоснована необходимость выделения психической неприкосновенности как самостоятельного объекта правовой защиты, отличного от защиты физической неприкосновенности. Впервые исследованы особенности нейрохакинга в контексте метавселенной и технологий искусственного интеллекта, включая анализ новых типов атак и угроз нейробезопасности.

Практическая значимость: результаты исследования имеют важное значение для развития правового регулирования в области нейробезопасности и разработки соответствующих нормативных актов. Выявленные типы нейропреступлений и их классификация могут служить основой для создания специализированного законодательства о защите нейронных данных и психической неприкосновенности. Практические рекомендации по обеспечению нейробезопасности интерфейсов «мозг – компьютер» востребованы в медицинской практике, индустрии видеоигр, системах аутентификации и разработке приложений для смартфонов.

Для цитирования

Коэльо, Д. П. (2025). Нейрохакинг в эпоху цифровизации и искусственного интеллекта: правовые аспекты защиты нейронной информации. *Journal of Digital Technologies and Law*, *3*(3), 397–430. https://doi.org/10.21202/jdtl.2025.16

Содержание

Введение
1. От киберпреступности к нейропреступности
   1.1. Связь между киберпреступностью и нейропреступностью
   1.2. Концепция интерфейса «мозг – компьютер» и примеры его использования
   1.3. Различия между нейронными и психическими манипуляциями
   1.4. Правовая автономия преступлений против психической целостности в сравнении с преступлениями против физической целостности
2. От киберпреступности к нейрохакингу
   2.1. Прототипы нейропреступлений, которые обычно относят к нейрохакингу
   2.2. Понятие нейрохакинга
   2.3. Нейрохакинг на основе различных типов приложений интерфейса «мозг – компьютер»
      2.3.1. Масштаб проблемы
      2.3.2. Приложения интерфейса «мозг – компьютер», которые могут стать целью нейрохакинга

2.4. Модальности нейрохакинга, основанные на четырехчастном цикле интерфейса «мозг – компьютер»
2.4.1. Масштаб проблемы
2.4.2. Манипуляции на этапе ввода нейронной информации
2.4.3. Манипуляции на этапе измерения и записи мозговой активности
2.4.4. Манипуляции на этапе декодирования и классификации нейронной информации
2.4.5. Манипуляции на этапе вывода результата
3. Нейрохакинг в эпоху цифровизации и искусственного интеллекта
3.1. Концепция эпохи цифровизации и искусственного интеллекта
3.2. Концепция метавселенной
3.3. Цифровое сенсорное взаимодействие в метавселенной
3.4. Интерфейс «мозг – компьютер» в метавселенной
3.5. Нейрохакинг в метавселенной
3.6. Интерфейс «мозг – компьютер» на основе искусственного интеллекта
3.7. Нейрохакинг и искусственный интеллект
Заключение
Список литературы

Введение

Есть мнение, что незаконный доступ к нейронной информации или манипулирование ею невозможны и никогда не будут осуществимы в том виде, в котором это часто предполагается и которого опасаются[1]. Основной причиной этого является ограниченное понимание нейронного кода, т. е. языка, с помощью которого мозг кодирует и обрабатывает информацию. Чтобы это стало возможным, потребовалось бы расшифровать нейронный код для достижения конкретного результата (доступа или манипуляции) и среди миллиардов нейронов, существующих в человеческом мозге, определить, какой именно из них следует стимулировать[2]. В настоящее время ученые только представляют, какую область мозга стимулировать, однако определение конкретного нейрона по-прежнему остается недостижимой задачей. Кроме того, у разных субъектов за определенную функцию могут отвечать разные нейроны[3]. С другой стороны, есть мнение, что невозможно повлиять на поведение субъекта, стимулируя только один нейрон, поскольку функция мозга зависит от скоординированной активности сложных нейронных цепей, включающих сотни или миллиарды нейронов. Скоординированная стимуляция больших сетей нейронов с целью навязывания целенаправленного и специфического

1 Fields, R. D. (2022). Hacking the brain: More fantasy than reality. The UNESCO Courier. Should we be afraid of neuroscience? (p. 9). UNESCO. https://clck.ru/3Nkhbr

2 Там же.

3 Там же.

поведения в целях манипулирования и ментального контроля представляется практически невозможной[4].

В целом все может считаться системой, включая человеческий мозг. И, как и все системы, человеческий мозг также может являться объектом «взлома». Есть мнение[5], что человечество «взломало» законы природы[6]. Подсчет карт в блэкджеке – это взлом[7]. В большинстве видов спорта люди прибегают к «взлому». Так, в «Формуле-1» команды пытаются найти новые способы изменения дизайна автомобилей, которые прямо не запрещены регламентом[8]. Предвыборные махинации являются хакерством в политике[9]. Кроме того, в финансовом и деловом мире также используются различные методы взлома. Большинство игроков на рынке, от предпринимателей до финансовых учреждений, пытаются найти лазейки в системе (т. е. в законе) в основном для того, чтобы получить преимущество перед конкурентами. В частности, они используют ситуации, которые прямо не запрещены, но представляют собой намеренный (или нет) подрыв системы. Например, компании Uber[10] и Airbnb[11], как и другие крупные технологические корпорации (организации), всегда нарушали правила, установленные правовыми системами ряда юрисдикций. Таким образом, концепция «воспрепятствования», вероятно, так же стара, как и понятия «пробел в законе» или «пробел в системе», и так же стара, как сама человеческая цивилизация, поскольку и человека, видимо, можно взломать. В этом контексте человеческий мозг представляет собой систему, которая, появившись как средство выживания и, прежде всего, размножения, подвергалась оптимизации в результате непрерывного взаимодействия с окружающей средой на протяжении миллионов лет.

---

4 Там же.

5 Schneier, B. (2021). The Coming AI Hackers. Belfer Center for Science and International Affairs. Harvard Kennedy School. https://clck.ru/3Nkhe4

6 Английское слово hacker обычно переводится на другие языки как «компьютерный пират». Однако использование такого перевода слова представляется неточным. Хакер может действовать как «пират», а «пират» может действовать как «хакер», но эти два определения, по-видимому, не эквивалентны. Скорее, они просто дополняют друг друга. Хакеры используют системы, будь то на компьютере, в телефоне, при личном общении или в любом другом аспекте человеческой жизни. Как правило, они действуют законными способами. Хакеры (или «взломщики») незаконно пытаются расшифровать (взломать) систему ради развлечения либо для получения определенного результата или преимущества. Несмотря на проблемы с семантикой и терминологическую путаницу, в данной статье в основном будет использоваться термин «хакер», потому что он наиболее известен, а также для легкости чтения. См. Ribeiro, J. B. (2019, 12 Fevereiro). 'Hacker' vs 'Pirata Informático': a riqueza de uma definição perdida na tradução. SH/FTER. https://clck.ru/3NkhkJ

7 Keating, S. (2022). How a magician-mathematician revealed a casino loophole. BBC. https://clck.ru/3Nkhnx

8 Straw, E. (2022, February 22). F1's new philosophy in combatting design loopholes. The Race. https://clck.ru/3Nkhq9

9 Ax, J. (2023). North Carolina court allows partisan gerrymandering. Reuters. https://clck.ru/3Nkhrs

10 Henley, J. (2017, September 29). Uber clashes with regulators in cities around the world. The Guardian. https://clck.ru/3Nkht2

11 Neubauer, I. L. (2019, August 30). Countries that are cracking down on Airbnb. The New Daily. https://goo.su/UcOHh

Таким образом, когнитивный хакинг, по-видимому, является мощным инструментом[12] в отношениях между людьми, и одной из его разновидностей является техника манипулирования, известная как «социальная инженерия». В области киберпреступности единственное новшество заключается в использовании технологий для взлома, потому что компьютеры, как и человеческий мозг, также являются системами. За последние несколько десятилетий мы стали свидетелями того, как методы взлома адаптировались к компьютеризации традиционных систем. Эта компьютеризация, по-видимому, изменила методы взлома в трех аспектах: масштаб, охват и скорость. Во-первых, она усилила и расширила характер взломов, тем самым увеличив их масштабы. Во-вторых, растущее число разработок программного и аппаратного обеспечения позволило системам развиваться быстрее, чем предполагалось изначально. Скорость работы компьютеров не отставала от этого развития, что также способствовало использованию методов взлома[13]. С переходом от Web 1.0 к Web 2.0 и Web 3.0, а в последнее время и к Web 4.0 появились новые прорывные технологии[14], и использование цифровых или искусственных компьютерных систем расширяется все более быстрыми темпами (Ienca & Haselager, 2016)[15]. В конечном счете с развитием киберпреступности методы взлома сосредоточатся на человеческом

---

12 Schneier, B. (2021). The Coming AI Hackers. Belfer Center for Science and International Affairs. Harvard Kennedy School. https://clck.ru/3Nkhe4. Например, многие из влиятельных социальных систем, составляющих основу общества, такие как демократия и рыночная экономика, зависят от решений, принимаемых людьми. Этот процесс может стать объектом когнитивного взлома, например, через социальные коммуникации. Современная реклама, персонализированная в соответствии с нашими предпочтениями и поведением, представляет собой своего рода массовый взлом человеческого мозга, в частности сознательных психических процессов, включая предшествующее бессознательное состояние. То же относится к дезинформации (часто распространяемой самими СМИ), которая разрушает общепринятое представление о реальности. Постоянное использование таких терминов, как «терроризм» или «кибертерроризм», в средствах массовой информации и в выступлениях политиков также представляет собой взлом когнитивной системы с целью убедить людей в том, что это более серьезная угроза, чем она есть на самом деле, и тем самым вызвать страх и исказить оценку риска.

13 Schneier, B. (2021). The Coming AI Hackers. Belfer Center for Science and International Affairs. Harvard Kennedy School. https://clck.ru/3Nkhe4

14 Термин «прорывные технологии» появился относительно недавно. Он подразумевает изменение стандартов, моделей или технологий, уже существующих на рынке. Другими словами, технологическая инновация, продукт или услуга с так называемыми прорывными характеристиками отличаются разнообразием, революционностью, новаторством, они никогда не рассматривались и не применялись в данном контексте. См. Dufloth, R. (2017). Novas tecnologias e o futuro do profissional do Direito. Mgalhas. https://clck.ru/3Nm3jy

15 В целом технологии, связанные с Web 1.0, Web 2.0, Web 3.0 и Web 4.0, позволяют пользователям напрямую взаимодействовать с данными и системами и могут использоваться для решения широкого спектра повседневных и профессиональных задач. Например, системы GPS помогают в геолокации и пространственной навигации, портативные устройства отслеживают такие процессы организма, как частота сердечных сокращений, потребление калорий и снижение веса. Также в качестве примера можно привести персональные компьютеры, которые помогают в решении когнитивных задач, таких как арифметические вычисления, создание письменных текстов и запоминание информации. Цифровые активы на основе блокчейна позволяют осуществлять международные транзакции в считаные минуты или даже секунды, а системы искусственного интеллекта позволяют мгновенно создавать оригинальные тексты, изображения или видеоролики. См. Nath, K. (2022). Evolution of the Internet Web 1.0 to Metaverse: The Good, the Bad and the Ugly. Research Gate. https://clck.ru/3NkiAo

мозге и психике как таковой, в частности, в форме «нейропреступлений» и «нейрохакинга» (также обычно называемого взломом мозга). При таком сценарии увеличение масштабов, сферы применения и скорости методов взлома будет становиться все более заметным.

Цель работы – внести вклад в изучение и первоначальное формулирование предмета, понимание которого никогда не будет достаточным не в последнюю очередь из-за высокого уровня юридических активов, о которых идет речь.

1. От киберпреступности к нейропреступности

1.1. Связь между киберпреступностью и нейропреступностью

Общепринятого определения киберпреступности не существует. Термины «киберпреступность», «компьютерная преступность», «преступления, связанные с использованием компьютеров» или «преступления, связанные с использованием высоких технологий» используются часто, но достаточно произвольно. На международном, общеевропейском или национальном уровне нет единого мнения относительно формулировок, определений, типологии или классификации киберпреступности (Rodrigues, 2009; Vasconcelos Casimiro, 2000). Четкого определения понятий «киберпреступность» или «компьютерное преступление» нет и в португальском законодательстве[16]. В литературе и юриспруденции также нет единообразной концепции (Venâncio, 2011). Отсутствие единообразия проявляется в том, что термин «киберпреступность» в общем и абстрактном виде охватывает целый ряд преступлений, совершаемых с использованием информационно-коммуникационных технологий. Этот термин включает как классические преступные деяния, так и новые виды преступлений.

По мнению Европейской комиссии, киберпреступления – это «преступные действия, совершаемые с использованием сетей электронных коммуникаций и информационных систем или против таких сетей и систем»[17]. Такие преступления делятся на три вида. Во-первых, это традиционные формы преступной деятельности, но использующие Интернет (включая кражу идентичности и фишинг) для совершения преступлений (например, компьютерное мошенничество или спуфинг). К этим традиционным формам также относится международная электронная торговля наркотиками, оружием и видами животных, находящимися под угрозой исчезновения. Во-вторых, к киберпреступлениям относится публикация в Интернете незаконного контента, такого как материалы, подстрекающие к терроризму, насилию, расизму и ксенофобии или сексуальному насилию над несовершеннолетними. И, наконец, это преступления, совершаемые исключительно в электронных сетях; они представляют собой новые и часто крупномасштабные деяния, которые были «неизвестны в эпоху

[16] Например, в Португалии в дополнение к видам преступлений, предусмотренным Законом № 109/2009 от 15 сентября, который развивает положения национального законодательства о киберпреступности (https://clck.ru/3Nkxa7), другие виды преступлений подобного рода предусмотрены в Уголовном кодексе Португалии и в различных других отдельных правовых источниках.

[17] European Commission. (2007). Towards a general policy on the fight against cyber crime. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. https://clck.ru/3NkiNh

до Интернета». В последнем случае преступные агенты атакуют системы или целые информационные инфраструктуры и даже конфиденциальную государственную информацию (что представляет собой национальную угрозу). При этом, по данным Европейской комиссии, эти атаки могут осуществляться через «ботнеты» (сеть роботов), т. е. преступные агенты распространяют вредоносное программное обеспечение (ПО), которое превращает компьютер пользователя в бота. Зараженная сеть или информационная инфраструктура используются для совершения преступлений без ведома их пользователей. Итак, компьютерное преступление представляет собой любое деяние, в ходе которого компьютер или аналогичная технология либо служит средством достижения преступной цели, либо представляет собой лишь символическую цель этого деяния или даже объект преступления (Marques & Martins, 2006). Поэтому необходимо проводить различие между «компьютерным преступлением», при котором объектом преступления являются информационные технологии, и «преступлением, совершенным с использованием компьютерных средств», когда информационные технологии являются средством совершения преступления.

По этой логике, если преступление совершается с использованием нейронных интерфейсов и, помимо того, что представляет физическую угрозу для пользователей, также оказывает глубокое влияние на их поведение и самовосприятие, мы имеем дело с «нейропреступлением»[18]. Особую актуальность приобретает неправомерное использование информационных технологий в контексте нейротехнологий, поскольку они применяются (прямо или косвенно) к работе мозга, одного из самых важных органов человека. Человеческий мозг не только вносит значительный вклад в жизненные процессы, такие как размножение и поддержание жизни, но и обеспечивает сознание, восприятие, способность мыслить и рассуждать, память и речь. Кроме того, он по-прежнему имеет огромное значение для поведения человека и его самовосприятия как существа или индивидуума, наделенного чувствами и эмоциями (Ienca & Haselager, 2016). Таким образом, нейропреступление можно определить как любое деяние, в котором человеческий мозг и/или психика служит средством достижения преступной цели либо является символической целью этого деяния или объектом преступления. Следовательно, необходимо проводить различие между «нейропреступлением», при котором мозг и/или психика прямо или косвенно являются объектом преступления, и «преступлением, совершенным с использованием нейронных и/или психических манипуляций», при котором мозг и/или психика являются средством совершения преступления. Таким образом, как мы увидим в п. 3 этого раздела, необходимо также проводить различие между нейронными манипуляциями и чисто психическими манипуляциями. Кроме того, при нейропреступлении может совершаться не прямой, а лишь косвенный доступ к мозгу или сохраненной информации. Например, функции нейронного устройства могут быть ограничены, модифицированы или разрегулированы. С учетом современных достижений в области технологий нейронной инженерии (в основном реализуемых в секторе здравоохранения) этот сценарий становится все более реальным. В этом случае преступник воздействует на мозг жертвы косвенно, поскольку во время атаки не осуществляется прямой доступ к нейронной системе и значительные манипуляции с ней не производятся. Тем не

[18] Данный термин обычно относится к преступной деятельности, совершаемой с использованием нейронных устройств.

менее психическое состояние жертвы подвергается существенному влиянию, например, поведение ограничивается или сковывается, наступает эмоциональная реакция в виде паники, страха или психологических расстройств, возникают травмирующие воспоминания. Стоит отметить, что при определенных обстоятельствах исполнитель и объект преступления меняются ролями. Например, пользователи с психической нестабильностью могут повредить свои нейронные устройства, чтобы совершить попытку самоубийства (Ienca & Haselager, 2016). Таким образом, в широком смысле понятие нейропреступления можно определить как преступление против разума человека или группы людей, совершаемое с использованием нейронных и/или чисто психических манипуляций с помощью нейронного устройства и с намерением прямо или косвенно причинить физический или психический вред, включая ущерб репутации и/или имуществу.

В области нейропреступности и нейронной стимуляции в настоящее время считаются особенно важными два типа нейронных устройств. Во-первых, это стимуляторы мозговой активности, особенно системы глубокой стимуляции мозга (deep brain stimulation, DBS) и транскраниальной стимуляции постоянным током (transcranial direct current stimulation, tDCS). Во-вторых, это интерфейсы «мозг – компьютер» (brain-computer interface, BCI). Оба типа устройств обеспечивают прямой доступ к нейронным вычислениям, хотя и разными способами (моделирование мозга или считывание активности мозга). Кроме того, они доступны не только как медицинские технологии, но и как продукты, предназначенные для условно здоровых пользователей. Поэтому эти устройства вызывают многочисленные вопросы с точки зрения «нейробезопасности». Фактически на сегодняшний день основными нейронными устройствами, используемыми для взлома (даже при наличии экспериментальных данных и в контексте реальных ситуаций), являются интерфейсы «мозг – компьютер», поэтому мы рассмотрим только эти устройства (Ienca & Haselager, 2016).

1.2. Концепция интерфейса «мозг – компьютер» и примеры его использования

В отличие от простых нейростимуляторов (электронных устройств, подобных кардиостимуляторам) интерфейсы «мозг – компьютер» (далее – ИМК) используются не для стимуляции мозга, а для установления прямого канала связи, который, минуя периферическую нервную систему и мышцы, позволяет пользователям управлять внешним компьютером исключительно посредством мозговой активности (Ienca & Haselager, 2016; Vallabhaneni et al., 2005). Они впервые появились в области клинической медицины как терапевтическая технология для оказания медицинской помощи неврологическим пациентам. В клиническом контексте приложения ИМК используются для восстановления, поддержания и усиления двигательных, когнитивных или сенсорных функций у пациентов, страдающих неврологическими расстройствами, которые непосредственно влияют на развитие моторики и/или когнитивные и сенсорные функции, включая травмы спинного мозга, инсульты и неврологические двигательные заболевания, такие как боковой амиотрофический склероз (БАС) и мышечная дистрофия (Ienca & Haselager, 2016).

ИМК делятся на два типа: инвазивные и неинвазивные. Инвазивные ИМК требуют хирургической имплантации электродных решеток в центральную нервную систему или простого прямого подключения. Неинвазивные ИМК регистрируют

мозговую активность с помощью электродов, расположенных снаружи черепа, т. е. с помощью технологий нейровизуализации, таких как электроэнцефалография (далее – ЭЭГ) и электромиография. В обоих случаях устанавливается прямое взаимодействие между мозгом пользователя и нейронным устройством. Как правило, это взаимодействие представляет собой четырехфазный цикл (Ienca & Haselager, 2016; Van Gerven et al., 2009; Bernal et al., 2022)[19]. Первая фаза состоит из ввода нейронной информации (т. е. создания определенной мозговой активности) пользователем в ответ на заданный стимул (всякий раз, когда пользователь ИМК хочет выполнить определенную умственную задачу или достичь определенного когнитивного состояния). Вторая фаза включает измерения и регистрацию мозговой активности. На этом этапе интерфейс обнаруживает, измеряет и записывает паттерны мозговой активности пользователя во время когнитивного процесса или выполнения определенной умственной задачи. На третьем этапе необработанные нейронные данные (нейронная информация), полученные в результате второго этапа, декодируются, чтобы оценить их основные характеристики и классифицировать. После декодирования и классификации данные преобразуются в определенные выходные данные, необходимые пользователю. В целом результатом четвертого этапа является выполнение действий, изначально запланированных, желаемых или считающихся полезными для пользователя, посредством управления приложениями, подключенными к ИМК. Управляемые приложения представляют собой устройства с электроприводом, такие как электрические инвалидные кресла или роботизированные протезы конечностей, сенсорные устройства и другие типы программных и аппаратных приложений (включая мобильные приложения и сотовые телефоны). По завершении каждого из этапов пользователь может увидеть достигнутый результат и приступить к следующему этапу (Ienca & Haselager, 2016). Примером применения этих технологий является Герт Ян Оскам, который после аварии на мотоцикле более десяти лет страдал параличом нижних конечностей, но теперь снова может ходить с помощью ИМК (хотя пока и не вполне свободно)[20].

Сегодня приложения ИМК доступны не только в клинических условиях, но и для широких слоев населения (Mochan et al., 2025). На рынке появилось множество коммерческих приложений для ИМК-устройств на основе ЭЭГ, которые становятся все более популярными как в сфере видеоигр, так и для повседневной деятельности (Ienca & Haselager, 2016)[21]. ИМК используются также в индустрии электронных телекоммуникаций. Так, некоторые мобильные приложения (например, приложение Xwave, выпущенное более 10 лет назад!) позволяют устанавливать прямое соединение с совместимыми мобильными телефонами iPhone через определенные

---

[19] В этой связи следует отметить, что ИМК могут быть классифицированы в зависимости от степени их инвазивности. В неинвазивных системах электроды размещаются на коже головы, тогда как инвазивные системы требуют хирургической процедуры для размещения электродов внутри черепа – либо на поверхности головного мозга, либо даже внутри самого мозга.

[20] Whang, O. (2023). Brain Implants Allow Paralyzed Man to Walk Using His Thoughts. https://clck.ru/3Nkxhk

[21] Например, см. веб-сайты компаний Emotiv Inc. и Neurosky Inc., которые являются пионерами в области коммерциализации неинвазивных, интуитивно понятных и доступных ИМК для видеоигр, интерактивного телевидения и систем управления: https://clck.ru/3NkiYN и https://clck.ru/3NkiZy См. также Gordon, L. (2020, December 16). Brain-controlled gaming exists, though ethical questions loom over the tech. The Washington Post. https://clck.ru/3Nkicf

типы наушников и записывать мозговые волны (Ienca & Haselager, 2016)[22]. Сектор вооружений в настоящее время также разрабатывает несколько приложений ИМК (Ienca & Haselager, 2016; Czech, 2021). Например, Агентство перспективных исследовательских проектов Министерства обороны США (DARPA) финансирует широкий спектр проектов в области ИМК, в основном направленных на восстановление поведенческих или нейронных функций у солдат, а также на улучшение подготовки и результативности военнослужащих и агентов секретных служб (Ienca & Haselager, 2016; Kotchetkov et al., 2010; Miranda et al., 2015). Основываясь на огромном потенциале управления мозгом с помощью нейронных вычислительных устройств и учитывая возможные преимущества и базовую функциональность, можно прогнозировать, что ИМК постепенно заменит клавиатуру, сенсорный экран, компьютерную мышь и даже технологию голосовой поддержки, поскольку потребители смогут взаимодействовать непосредственно с компьютерами (Ienca & Haselager, 2016; Yuan et al., 2010; Radu, 2024). Однако, как мы покажем ниже, хотя потенциальные выгоды от ожидаемой массовой коммерциализации определенных клинических и неклинических применений технологии ИМК представляются значительными и хорошо изученными, остаются в значительной степени не изученными очень серьезные (и, возможно, непоправимые) риски, связанные с нейробезопасностью. Чтобы понять эти риски, необходимо сначала провести различие между нейронными и чисто психическими манипуляциями.

1.3. Различия между нейронными и психическими манипуляциями

После более чем 2000 лет философских споров и самых последних впечатляющих научных достижений в области искусственного интеллекта (далее – ИИ) и обработки данных проблема дуализма сознания и мозга сохраняется и по-прежнему не поддается однозначному решению (Bublitz & Merkel, 2014; Moulin, 2022). По словам Maria Fernanda Palma, абсолютное отрицание дуализма сознания и мозга или сведение феноменов сознания к состояниям мозга может оказать значительное влияние на реальные поведенческие основания юридической ответственности; особенно это касается добровольных действий или истинной способности отдельных лиц считаться виновными по уголовному закону[23]. Если акт сознания не предшествует принятию решения, то неизбежно ставится под сомнение такой критерий возникновения или усиления ответственности за намеренное деяние, как свободное и осознанное решение. В этом смысле абсолютное самоопределение человека как источника ответственности ставится под сомнение, если предположить, что разумное решение может быть вычислено подобно алгоритму и имитировано с помощью математических процессов. Нейробиология, по-видимому, предлагает натуралистическую редукцию разума и состояний сознания, тогда как наука о данных и искусственном интеллекте рассматривает функционирование мозга как автономный биологический процесс, в котором могут воспроизводиться психические состояния и их связь с поведением человека. Эта точка зрения неожиданно приводит к переосмыслению дуалистической

[22] PLX Devices Inc. XWave – Mind Interface Introduction and Teaser. 2010. https://clck.ru/3NkifC

[23] Fernanda Palma, M. (2021–2022). Ciberneurodireito. Powerpoint Presentation. Short Course in Criminal Law on Artificial Intelligence and Artificial Intelligence in Criminal Law. FDUL. IDPCC/ CIDPCC, 4.

гипотезы, рассматривающей мозг всего лишь как одну из возможных основ человеческого поведения. Право как таковое, а также в его связях со смежными науками направлено на изучение того, имеет ли конкретное психическое состояние причинно-следственную связь с работой мозга и обязательно ли оно подразумевает определенное поведение, а также в какой степени оно поддается контролю[24].

По мнению Jan Christoph Bublitz и Reinhard Merkel, все психические явления так или иначе связаны с деятельностью мозга. Это дает основания утверждать, что законодателю следует проявлять осторожность при описании отношений между сознанием и мозгом как дуалистических; не в последнюю очередь причина этого в том, что трудно идентифицировать изменения в психическом состоянии, не выявив также определенных изменений на церебральном (нейронном) уровне. Также утверждают, что психические состояния не только коррелируют с определенным состоянием мозга, но и вызываются или осознаются на основе определенного физического состояния. Однако всякий раз, когда рассматривается более точное и конкретное описание этой корреляции, возникает множество проблем, поскольку нет единого мнения относительно связи с причинами или процессом «осознания» (Bublitz & Merkel, 2014). Таким образом, несмотря на существующую в настоящее время в психиатрии тенденцию классифицировать любое психическое расстройство как расстройство головного мозга в строгом смысле этого слова, некоторые ученые утверждают, что психические травмы не обязательно связаны с физическими нарушениями. В принципе, это не мозг «решает», «страдает» или ощущает «моральный ущерб». Напротив, все указывает на то, что мы имеем дело с психическими состояниями/процессами людей, а не с качествами физических объектов. Для нормативных целей, связанных с понятиями «вред» или «расстройство/дисфункция», можно считать доказанным, что психика и мозг заслуживают индивидуального внимания (Bublitz & Merkel, 2014). Например, психические расстройства/дисфункции, по-видимому, являются результатом определенных психологических функций или связаны с определенными социальными нормами, а не с электрохимическими процессами в мозге. В данном случае мы имеем дело с психическими и поведенческими феноменами, которые невозможно описать исключительно в терминах неврологии. Например, депрессию принято считать специфическим психическим симптомом, и страдание от депрессии зависит исключительно от проявления этого симптома. Даже если бы было известно (а это не так), что все симптомы депрессии тесно связаны с химическим дисбалансом на уровне нейромедиаторов, различие между психической и мозговой дисфункцией сохранялось бы (Bublitz & Merkel, 2014). Исходя из этой логики, было показано, что психические нарушения нельзя лечить так же, как повреждения головного мозга. В противном случае можно было бы забыть обо всех достижениях современного уголовного права и принять римскую концепцию иниурии, которая охватывала любые преступления, совершенные против личности. Таким образом, специалисты высказываются за определение психических состояний, подлежащих правовой защите и за введение конкретных нормативных положений, предусматривающих наказание за посягательство на психическую неприкосновенность, а не за адаптацию и расширение защиты физической неприкосновенности.

[24] Fernanda Palma, M. (2021–2022). Ciberneurodireito. Powerpoint Presentation. Short Course in Criminal Law on Artificial Intelligence and Artificial Intelligence in Criminal Law. FDUL. IDPCC/ CIDPCC, 4. Pp. 6–14.

В то время как понятие неприкосновенности мозга должно охватывать физические вмешательства, т. е. повреждение мозга (независимо от психических последствий), понятие психической неприкосновенности должно охватывать психические вмешательства, т. е. психические повреждения независимо от последствий для мозга (Bublitz & Merkel, 2014).

В этой связи также утверждается, что психическая неприкосновенность должна предусматривать защиту от психологических манипуляций/вмешательств, таких как провоцирование эмоций, манипулирование предпочтениями и процессами принятия решений, оптимизация неконсенсусного неврологического развития, манипулирование памятью и волей, другие когнитивные и эмоциональные феномены (Bublitz & Merkel, 2014). Во всех этих случаях манипуляции/вмешательства ограничивают возможности психики или изменяют личные предпочтения и волевые функции. Однако на сегодняшний день ни одна из этих манипуляций/вмешательств, по-видимому, в целом не подпадает под действие правил, защищающих физическую неприкосновенность и психическое здоровье. Причина этого не в последнюю очередь в том, что все эти манипуляции/вмешательства вызывают только психологические изменения и не отвечают критериям причинения физического вреда. Поскольку жертва не страдает от каких-либо повреждений головного мозга и не испытывает физической боли или дискомфорта, незаконность этих манипуляций/вмешательств обусловлена их чисто психологическими последствиями (Bublitz & Merkel, 2014). В условиях развития цифровых технологий и искусственного интеллекта все указывает на то, что в будущем нейробиологические доказательства будут играть все более важную роль в установлении и раскрытии истины в случае судебных разбирательств, связанных с мозгом и психической целостностью (Shen, 2013). При этом не имеет значения, сохранится ли отрицание дуализма сознания и мозга. По этой причине, прежде чем мы перейдем к анализу нейрохакинга как такового, необходимо высказать некоторые соображения относительно текущего обсуждения юридической автономии преступлений против психической целостности и преступлений против физической неприкосновенности.

1.4. Правовая автономия преступлений против психической целостности в сравнении с преступлениями против физической целостности

Как было показано в предыдущем разделе, нейробиология и наука о данных и искусственном интеллекте не только подвергают сомнению предположения о роли психики в естественном мире, но и побуждают к переосмыслению ее роли в мире права. Получается, что в настоящее время закон обеспечивает одностороннюю защиту, поскольку он систематически защищает тело и мозг и лишь фрагментарно – разум и психические состояния. Как объяснялось в предыдущем разделе, фундаментальный вопрос заключается в том, в какой степени возможно законное вмешательство в сознание и психические состояния других субъектов. В связи с коммерциализацией и массовым внедрением нейронных технологий, способных воздействовать на сознание и обнаруживать психическую активность, многие специалисты утверждают, что закон должен предусматривать автономную и индивидуальную правовую защиту психической неприкосновенности (Bublitz & Merkel, 2014; Abegão Alves, 2020). Эта научно-философская и юридическая дискуссия в основном сосредоточена на двух аспектах: (i) рассмотрении эмпирической и концептуальной автономии

психического по отношению к физическому; (ii) рассмотрении юридической автономии преступлений против психической неприкосновенности по отношению к преступлениям против физической неприкосновенности. Так, в Институте уголовного права и криминологических наук юридического факультета Лиссабонского университета ведется научный проект «Преступления против психики» (инициированный после публикации новаторского исследования Bublitz & Merkel, 2014), целью которого является восполнение этого пробела в правовом мышлении. Исследование показало, что юристы и мыслители в области права пока не установили пределов законного изменения психического состояния других людей, так что проблемы регулирования реальности по-прежнему опережают развитие юридической науки. Также, согласно этому проекту, самые последние научные открытия требуют внимания закона не только с точки зрения агрессора/преступника, но и с точки зрения жертвы. В связи с этими открытиями юридическая наука должна обсуждать как проблему свободы воли, так и основания уголовной ответственности, а также вопросы законных активов, подлежащих защите. Именно этот второй аспект значимости нейробиологии для юриспруденции еще предстоит изучить. В этом смысле текущая задача состоит в том, чтобы углубить научно-философские и юридические дебаты по этому вопросу как на национальном, так и на международном уровне. В частности, необходимо проблематизировать ключевые вопросы, предлагая решения и возможные пути для будущих исследований, которые неизбежно будут находиться на пересечении различных областей знаний.

2. От киберпреступности к нейрохакингу

2.1. Прототипы нейропреступлений, которые обычно относят к нейрохакингу

За последние несколько лет было выявлено множество видов нейропреступлений, обычно называемых нейрохакингом. К ним относятся взлом программного обеспечения беспроводных протезов конечностей, злонамеренное перепрограммирование устройств нейростимуляционной терапии (т. е. несанкционированное беспроводное изменение конфигурации устройства с целью генерирования определенных мозговых стимулов) и несанкционированный перехват сигналов мозговых имплантатов с целью получения частной нейронной информации (Ienca & Haselager, 2016)[25]. Все это может быть выполнено только с использованием нейронных устройств, которые позволяют установить прямую связь с мозгом, таких как tDCS и особенно все более усовершенствуемый ИМК (Denning et al., 2009). Это прототипы нейропреступлений, которые обычно называют нейрохакингом. Далее мы покажем, что способ их осуществления очень похож на компьютерный взлом в контексте киберпреступности, как описано в разделе 1.1 о связи между киберпреступностью и нейропреступностью (Ienca & Haselager, 2016).

2.2. Понятие нейрохакинга

[25] Этот последний пример описывает специфический нейрокриминальный феномен, при котором атака направлена не просто на вывод нейронного устройства из строя, но и на получение несанкционированного доступа к частной информации.

В широком смысле нейрохакинг можно определить как неправомерное и злонамеренное использование нейронных устройств с целью незаконного получения нейронной информации и возможного манипулирования ею (Ienca & Haselager, 2016). Строго говоря, нейрохакинг представляет собой нейроатаку, осуществляемую с помощью нейронных устройств, в ходе которой злоумышленники получают незаконный доступ к нейронной информации, которой, в свою очередь, можно манипулировать, чтобы контролировать когнитивный процесс или выполнение определенной умственной задачи пользователем устройства. После того как доступ к нейронному устройству получен, оно используется для совершения преступлений с ведома пользователя или без него.

2.3. Нейрохакинг на основе различных типов приложений интерфейса «мозг – компьютер»

2.3.1. Масштаб проблемы

Как уже говорилось, ИМК могут быть перехвачены для обнаружения скрытой автобиографической информации пользователей с высокой степенью точности (Ienca & Haselager, 2016; Rosenfeld et al., 2006; Rosenfeld, 2011). Было показано, что перехваченный ИМК дает доступ к личной и конфиденциальной информации пользователей, например, PIN-кодам, данным банковских и кредитных карт, дате рождения, домашнему адресу, фотоснимкам знакомых им людей (Ienca & Haselager, 2016). Таким образом, фантастическое будущее уже не кажется вымыслом. Уже сейчас можно получать доступ к нейронной информации других людей и манипулировать ею (Mochan et al., 2025). Ниже мы показываем, что если конструктивные и функциональные характеристики современных нейронных устройств, которые все еще находятся в стадии разработки, не будут соответствовать строгим мерам нейробезопасности, их неправомерное и злонамеренное использование несет серьезные риски с точки зрения общественной безопасности (Ienca & Haselager, 2016)[26].

2.3.2. Приложения интерфейса «мозг – компьютер», которые могут стать целью нейрохакинга

Как было показано в разделе 2.1, в прототипах нейропреступлений используются нейронные устройства, позволяющие установить прямую связь с мозгом, а основными мишенями для взлома являются приложения ИМК. Выделяют четыре основных типа приложений ИМК, которые возможно использовать для нейрохакинга: (i) нейромедицинские приложения; (ii) приложения для аутентификации пользователей; (iii) видеоигры и развлечения и (iv) приложения на базе смартфонов. Для каждого из этих типов в настоящее время изучаются возможные сценарии атак, а также соответствующие меры нейробезопасности, которые необходимо применять (Mochan et al., 2025). На самом деле для некоторых приложений ИМК и соответствующих видов нейрохакинга уже имеются фактические данные и экспериментальные подтверждения их использования в реальных контекстах (Li et al., 2015). Как мы увидим в следующем

[26] Martinovic, I. et al. (2012). On the feasibility of side-channel attacks with brain-computer interfaces. USENIX security symposium. https://clck.ru/3NkoD5

разделе, в рамках этих четырех основных типов нейрохакинг может осуществляться на любой фазе цикла ИМК, описанных в разделе 1.2.

2.4. Модальности нейрохакинга, основанные на четырехчастном цикле интерфейса «мозг – компьютер»

2.4.1. Масштаб проблемы

Принимая во внимание описанные типы приложений ИМК, которые уже существуют в настоящее время (Mochan et al., 2025) и которые теоретически могут появиться в ближайшем будущем, рассмотрим, также теоретически, различные типы нейрохакинга, основанные на четырехфазном цикле ИМК. Напомним, что это фаза ввода нейронной информации, фаза измерения и регистрации мозговой активности, фаза декодирования и классификации нейронной информации и, наконец, фаза вывода (Ienca & Haselager, 2016).

2.4.2. Манипуляции на этапе ввода нейронной информации

При этом типе нейрохакинга хакер атакует пользователя ИМК в момент ввода нейронной информации, т. е. на первом этапе цикла. Вводом нейронной информации можно манипулировать, изменяя стимулы, передаваемые пользователю ИМК. Например, нейрохакеры могут заранее выбирать целевые стимулы, чтобы вызвать определенную реакцию у пользователя и таким образом облегчить доступ к его нейронной информации. Этот тип нейронных вредоносных программ имеет некоторое сходство со шпионскими программами на компьютере, поскольку они направлены на сбор информации о пользователе, отправку ее другому объекту и/или обеспечение контроля над компьютером или другим ИТ-устройством без разрешения или согласия пользователя (Ienca & Haselager, 2016). В этом случае вредоносное ПО, используемое для нейрохакинга, обладает способностью извлекать информацию непосредственно из сигналов, излучаемых мозгом, и поэтому широко известно как «программа-шпион для мозга». В будущем, по-видимому, появятся различные мобильные и портативные приложения для нейрошпионажа, и такие действия, как взлом паролей, кража личных данных, фишинг и другие виды нейронного мошенничества, будут все более распространенными (Ienca & Haselager, 2016). В настоящее время расшифровка сигналов мозга с уровнем точности и скорости, сравнимым с компьютерным взломом, возможна только в экспериментальной среде и лишь в ограниченных масштабах. Учитывая ограничения в плане расшифровки сигналов мозга, а также текущую степень зрелости рынка, вознаграждение для современного хакера, по-видимому, не стоит риска. Однако с развитием технологий и быстрым расширением рынка приложений для ИМК нейронная информация будет все больше цениться, а также появятся возможности для ее расшифровки (Ienca & Haselager, 2016).

2.4.3. Манипуляции на этапе измерения и записи мозговой активности

На этапе измерения и регистрации мозговой активности хакер атакует пользователя ИМК без его согласия или волеизъявления с целью получить результат, отличный от того, который ожидается при обычном функционировании нейронного устройства. Форма атаки может отличаться в зависимости от ее конкретной цели, при этом учитываются три основные цели: взлом исходных нейронных данных из ИМК (т. е. нейронной информации), нарушение функциональности и захват интерфейса

«мозг – компьютер». В целом взлом необработанных данных может вести к различным преступным действиям, направленным на ограничение определенного поведения пользователя нейронного устройства, нанесение вреда или использование преимуществ. Нарушение функциональности ИМК может производиться с целью манипулирования данными о мозговой активности, чтобы изменить, перегрузить или замедлить работу приложения ИМК. Хакер атакует канал связи интерфейса «мозг – компьютер», чтобы отслеживать или изменять данные, снизить или перехватить контроль пользователя над приложением ИМК. Во время взлома нейронное устройство получает приказы, которые расходятся с намерениями или желаниями его пользователя, и действует в интересах хакера. Например, нейрохакер может отключить устройство для воспроизведения речи, основанное на ИМК, чтобы заставить пользователя замолчать, или взломать интерфейс инвалидной коляски, чтобы определить маршрут пользователя (Ienca & Haselager, 2016).

2.4.4. Манипуляции на этапе декодирования и классификации нейронной информации

Нейрохакинг на этапе декодирования и классификации нейронной информации включает в себя манипулирование получением результата, ожидаемого пользователем, в процессе обычной обработки данных устройством ИМК. Это может быть сделано тремя различными способами: (i) путем добавления шума, что делает процесс декодирования излишне сложным; (ii) путем вмешательства в механизмы нейронного обучения и памяти (машинное обучение), чтобы изменить классификацию мозговых волн или (iii) путем замены волн, посылаемых по ИМК к устройству вывода. Каждый из этих методов имеет свои преимущества и недостатки. Например, добавление шума представляется наиболее простым в исполнении и наиболее трудным для обнаружения методом. Однако при его использовании шансы хакера на достижение желаемого результата снижаются. С другой стороны, два других метода более сложны в исполнении и их легче обнаружить, однако они обеспечивают максимальный контроль над системой ИМК. Как и при манипулировании фазой измерения и записи мозговой активности, хакер может манипулировать фазой декодирования и классификации, чтобы захватить контроль над устройством ИМК. При таком типе атаки цель состоит не только в том, чтобы ограничить или отобрать у пользователя контроль над устройством, но и в том, чтобы заменить его. Успешно взломав систему, хакер может получить частичный или полный контроль над устройством ИМК, одновременно ограничивая или устраняя контроль пользователя. В этом сценарии хакер получает возможность отслеживать, изменять или вставлять сообщения в канал связи ИМК (Ienca & Haselager, 2016).

2.4.5. Манипуляции на этапе вывода результата

В этом случае целью взлома является изменение результатов, воспринимаемых пользователем в конце цикла интерфейса «мозг – компьютер». Нейрохакер манипулирует восприятием непосредственно предшествующих действий или собственным самовосприятием пользователя, возникающим в результате когнитивных состояний, генерируемых ИМК. Преступный мотив, стоящий за этим типом взлома, заключается в том, чтобы без разрешения пользователя вызвать определенные когнитивные состояния или действия в последующем цикле (или во всех последующих

циклах) в интересах хакера. Например, нейрохакер может осуществлять своего рода «нейрофишинг»: заставить пользователя ввести определенный пароль или другой тип аутентификационной информации, чтобы начать или продолжить первоначально запланированный процесс. В этом случае, по-видимому, пользователь подвергается определенным травмирующим переживаниям. Преступные действия, которые подпадают под эту категорию, среди прочего включают мошенничество, фишинг, кражу личных данных и нанесение ущерба физической или психологической неприкосновенности (Ienca & Haselager, 2016).

3. Нейрохакинг в эпоху цифровизации и искусственного интеллекта

3.1. Концепция эпохи цифровизации и искусственного интеллекта

Эпохой информатизации обычно называют период 50–70-х гг. XX в., который характеризуется тем, что традиционные отрасли промышленности, созданные во время промышленной революции, трансформировались в экономику, основанную на информационных и коммуникационных технологиях. Сегодня, в начале XXI в., когда экономика переходит на цифровые технологии и искусственный интеллект, мы вступили в новый исторический период, а именно в эпоху цифровых технологий и искусственного интеллекта. Как упоминалось во введении, с развитием Web 1.0, Web 2.0 и Web 3.0, а в последнее время и Web 4.0 появились новые прорывные технологии, и использование цифровых и ИИ компьютерных систем расширяется все более быстрыми темпами. Среди этих новых прорывных технологий выделяются последние достижения в области иммерсивных технологий, метавселенных и виртуальных миров, а также в области искусственного интеллекта и науки о данных. В первой из этих областей выделяются технологии виртуальной (VR), дополненной (AR), смешанной (MR) и расширенной (RX) реальности, а также пространственные вычисления и цифровое сенсорное взаимодействие. Во второй области это в основном системы искусственного интеллекта и робототехники[27]. Обе эти области обещают произвести революционные изменения во взаимодействии общества и технологий. Эти типы технологий не только направлены на повышение эффективности взаимодействия с пользователями, но и обладают функциями и характеристиками, позволяющими развивать множество отраслей с головокружительной скоростью (Ford, 2016)[28] и темпами, превосходящими все прогнозы[29], в том числе в секторах, связанных с другими

[27] См. GPT-4. https://clck.ru/3NkoQK; Bing AI. https://clck.ru/3NkoTY; Gemini. https://clck.ru/3NkoV7. См. также достижения в области человекоподобных роботов, в частности: Boston Dynamics. https://clck.ru/3NkoY3; Tesla. https://clck.ru/3Nkxk8

[28] В этой связи следует отметить, что наиболее известным способом измерения прогресса в вычислительной мощности компьютеров является закон Мура. Гордон Э. Мур (Gordon E. Moore) предсказал, что каждые 18 месяцев количество транзисторов на микросхемах будет увеличиваться на 100 %. Однако информационные технологии выходят за рамки этого прогноза. Например, в отличие от аппаратного обеспечения, в котором значительно увеличился объем компьютерной памяти и объем цифровой информации, которую можно передавать по волоконно-оптическим кабелям, эффективность определенных алгоритмов в программном обеспечении растет темпами, превосходящими все прогнозы (Ford, 2016).

[29] Coelho, D. P. (2023). Os recentes avanços no setor da IA são uma benção ou uma maldição? Observador. https://clck.ru/3NkpED

прорывными достижениями, такими как облачные и передовые технологии, большие данные, квантовые вычисления, интерфейсы «мозг – компьютер», технологии распределенных реестров (такие как блокчейн), интернет вещей (IoT), умные города, распознавание лиц, робототехника и др.

Представьте, что эти технологии достигнут прогнозируемого потенциала (Dwivedi et al., 2022)[30]. В ближайшие 15–20 лет все процессы окажутся напрямую связаны. В метавселенной в цифровой форме будут созданы новые миры и страны[31]. Умные города будут подключены к интернету вещей, на каждом углу будут установлены камеры видеонаблюдения[32], оснащенные системами распознавания лиц и интеллектуальными сенсорными системами[33]. Дроны на базе искусственного интеллекта и гуманоидные роботы-полицейские будут патрулировать улицы и здания[34]. Университеты будут в основном работать на искусственном интеллекте[35]. В большинстве организаций не будет даже работников или физических помещений, поскольку они будут автономными, цифровыми и основанными на ИИ[36]. Бизнес в метавселенной станет цифровым и будет развиваться автономными цифровыми и ИИ-компаниями[37]. Промышленные роботы на базе ИИ будут производить все виды товаров[38]. Рабочие места будут практически полностью цифровыми[39]. Люди будут проводить практически весь свой день (и ночь) во все более развивающейся метавселенной[40]. Люди смогут по своему усмотрению выходить в физическую среду в виде голограмм, что позволит посещать собрания и рабочие места и даже свободно «перемещаться» в любую точку планеты[41]. И все это, разумеется, не выходя из

---

30 См. также Coelho, D. P. (2023). Ano 2050: Era Digital. Observador. https://clck.ru/3NkpRV; Chayka, K. (2021). We already live in Facebook's metaverse. The New Yorker. https://clck.ru/3NkjZb

31 См. Woodward, W. (2024). Backup nations: countries making digital twins to mitigate natural disasters. Nesta. https://goo.su/uVSUy; Widlund J. (2023) Singapore's First Country-Scale Digital Twin and The Future of Digital Open Data. https://clck.ru/3NkxqG

32 Также называемые телевидением замкнутого контура.

33 Davis, D. (2021). Facial Recognition And Beyond: Journalist Ventures Inside China's 'Surveillance State'. NPR. https://clck.ru/3NkjET

34 См. Jarecki, J., Wilson, N., & Trevellyan, K. (2024). Vermont police are using drones more than ever. Here's what that means. Vermont Public. https://clck.ru/3NkjGh ; Chen, H. (2023). Robôs com mais de 2 metros de altura integram força policial de Singapura em aeroporto. CNN Brazil. https://goo.su/W2x0

35 Carroll, M. (2024). UK's first 'teacherless' AI classroom set to open in London. Sky News. https://clck.ru/3NkjLK

36 Smith, T. (2024). Profitable, AI-powered companies with no employees to arrive 'next year'. Sifted. https://clck.ru/3NkjNX

37 Eckert, T., & Cigaina, M. (2023). The metaverse: A new space for business. SAP. https://clck.ru/3NkjPh

38 См. Ping, Ch. (2019) Robots to wipe out 20 million jobs around the world by 2030: Study. https://clck.ru/3Nkxtp; Semuels, A. (2020). Millions of Americans Have Lost Jobs in the Pandemic – And Robots and AI Are Replacing Them Faster Than Ever. Time. https://clck.ru/3Nkxxo

39 Hoover, A. (2024) The Metaverse Was Supposed to Be Your New Office. You're Still on Zoom. https://clck.ru/3Nky4S

40 Steele, C. (2022). People Are Spending More Time Online-and They're Not Happy About It. PC Mag. https://clck.ru/3NkzDa

41 См. Atkinson, E., & Meyer, M. (2022). Meeting in the Metaverse: The Future of Work?. University of Denver, Podcast. News. https://clck.ru/3Nkpxk. Verdict. In the metaverse, holograms offer more options than avatars. (2022, June 15). https://clck.ru/3Nkq2b

дома. Граница, отделяющая виртуальную реальность от дополненной и смешанной, станет менее выраженной, как и граница, отделяющая физическую реальность от цифровой. Цифровая валюта центрального банка станет единственным законным платежным средством[42]. В повседневных задачах людям будут помогать портативные и носимые технологии (во многих случаях невидимые)[43] или даже домашние роботы-гуманоиды, работающие на искусственном интеллекте[44]. В принятии решений будут участвовать голосовые помощники или даже технологии нейронного интерфейса, что позволит объединить человеческое сознание с искусственным интеллектом в своего рода симбиозе человека и машины[45]. Таким образом, при любом контакте человека с метавселенной будет инициироваться нейронная связь[46]. Цифровое сенсорное взаимодействие позволит людям чувствовать себя все более комфортно, подключаясь к метавселенной, и это реальность, которую новые поколения будут знать лучше всего. Человек всегда будет окружен камерами, микрофонами и интерфейсными системами. Даже эмбриональное развитие будет происходить в искусственных инкубаторах[47]. Многие предпочтут создавать и развивать эмоциональные или любовные отношения с домашними роботами-гуманоидами на основе искусственного интеллекта[48]. Домашних животных заменят искусственные питомцы[49]. Весь мир будет цифровым или основанным на искусственном интеллекте.

Само мышление станет небезопасным, потому что всякий раз, когда устанавливается связь с метавселенной и/или активируется технология нейронного интерфейса любого типа, человек становится открытой книгой. В этом случае использование компьютерных систем не ограничивается социальной, профессиональной и экономической сферами, а распространяется на психологическую и биологическую сферы. Ошеломляющая скорость развития этих областей, а также сочетание этих технологий неизбежно приведут к столь же ошеломляющему увеличению масштабов и скорости распространения киберпреступлений, нейропреступлений, а значит, и методов нейрохакинга. Таким образом, и как мы увидим в следующем разделе, исследования и инвестиции в кибербезопасность и нейробезопасность станут еще более актуальными (Pooyandeh et al., 2022).

---

42 Michel, N. (2024, June 17). CBDCs Are Instruments Of Control-And They're Here. Forbes. https://clck.ru/3Nkq5h

43 From Wearables to Implantables: The Rise of Invisible Technologies. https://clck.ru/3NkyPr

44 См. Reuters. (2024). A humanoid robot to help you around the house. https://clck.ru/3NkqCB; Schwartz, R. (2024). Is the world ready for Tesla's new domestic robots? The Week. https://clck.ru/3NkqE8

45 См. Brodsky, S. (2024, August 27). AI voice assistants evolve, promising deeper interaction. IBM. https://clck.ru/3NkqHZ; Niemeyer, K. (2024, August 3). Elon Musk says Neuralink could help humans compete with AI: 'Let's give people superpowers'. Business Insider. https://clck.ru/3NkqLa

46 How BCI can elevate the AR/VR experience. https://clck.ru/3NkyXe

47 Zimmer, K. (2021, March 30). The Ultimate Incubator: The Brave New World of Bionic Babies – Artificial placentas could improve the survival odds of premature infants. IEEE Spectrum. https://goo.su/PE2QYzM

48 См. Travers, M. (2024, March 24). A Psychologist Explains Why It's Possible To Fall In Love With AI. Forbes. https://clck.ru/3NkqXn; Chow, A. (2023). AI-Human Romances Are Flourishing-And This Is Just the Beginning. Time. https://clck.ru/3NkyiH

49 World Economic Forum. (2023). Moflin, an AI pet, responds like a real animal. https://clck.ru/3Nkqgf

3.2. Концепция метавселенной

В 1992 г. писатель-фантаст Нил Стивенсон в своем киберпанковском романе «Лавина» ввел термин «метавселенная». В нем он показывает трехмерный виртуальный мир, в котором люди, представленные в виде аватаров, взаимодействуют друг с другом и с искусственным интеллектом. В 2003 г. эта первоначальная концепция метавселенной (все еще далекая от концепции, идеализируемой в настоящее время) была впервые реализована в игре Second Life и даже имела некоторый успех[50]. Термин «метавселенная» образован путем сочетания греческого префикса «мета», который можно перевести как «запредельный» или «трансцендентный», и корня «verse», который происходит от слова «вселенная». Таким образом, мы имеем дело с миром, находящимся за пределами Вселенной (Bernal et al., 2022). Эта концепция направлена на представление виртуального (цифрового) мира, который, сосуществуя с физической реальностью (посредством дополненной реальности), позволяет нам преодолевать физические ограничения реального мира, такие как пространство и время. В этой цифровой среде (которая в будущем станет приобретать все большее значение) множество пользователей взаимодействуют друг с другом так же, как в реальной жизни, используя аватар, представляющий их цифровое альтер эго или их цифровую идентичность (Bernal et al., 2022). Таким образом, в широком смысле метавселенная состоит из пространства или набора виртуальных и совместно используемых пространств (обычно называемых цифровыми или виртуальными мирами или средами), к которым пользователи, представленные цифровыми аватарами, получают доступ и с которыми они взаимодействуют многомерным образом, используя гарнитуры или другие аксессуары. Другими словами, вместо простого просмотра контента пользователи могут погрузиться в него с помощью своих цифровых представлений[51].

Основными технологиями, которые в настоящее время составляют метавселенную и виртуальные миры, являются технологии погружения (виртуальная, дополненная, смешанная и расширенная реальность, ИМК и системы сенсорного взаимодействия), технологии 3D-моделирования и реконструкции, пространственные и пограничные вычисления, искусственный интеллект и наука о данных, IoT и технологии распределенного реестра (Pooyandeh et al., 2022)[52]. В отличие от современных технологий виртуальной и/или дополненной реальности, которые в основном используются для электронных игр или для замены клавиатуры, сенсорного экрана или компьютерной мыши, технологии будущего могут быть использованы для моделирования практически любой ситуации, связанной с физическим миром. Возможности

---

50 Second Life – это видеоигра, выпущенная в 2003 г., позволяет пользователям наслаждаться «второй жизнью» в виртуальном мире. Пользователи могут стать любой личностью и играть любую роль. В частности, они могут играть роль аватара в виртуальном мире, исследовать его, знакомиться с другими пользователями, принимать участие в индивидуальных и/или групповых мероприятиях и так далее, как это было бы в реальной жизни. См. веб-сайт видеоигры Second Life. https://clck.ru/3Nm4mQ

51 Pereira Coelho, D. (2021). Metaverse: should regulators be more attentive than ever? Observador. https://clck.ru/3Nm549

52 См. также Tucci, L. (2024, March 22). What is the metaverse? An explanation and in-depth guide. TechTarget. https://clck.ru/3Nkqqk

для взаимодействия будут охватывать самые разные сферы – от профессиональной деятельности до посещения виртуальных концертов[53] или просто приятного времяпрепровождения с друзьями. Таким образом, конечная цель состоит в том, чтобы устранить границы между физическим миром и виртуальной реальностью, позволяя пользователям взаимодействовать с виртуальными объектами через объекты физического мира и наоборот. В результате человек получает возможность обрабатывать любую информацию в режиме реального времени.

Используя технологию распределенного реестра, пользователи могут покупать и продавать невзаимозаменяемые криптоактивы с помощью взаимозаменяемых криптоактивов в метавселенной. Фактически в рамках «виртуального мира, основанного на блокчейне», функционирующего на основе «виртуальной экономики», криптоактивы, выпущенные с использованием технологии блокчейн, являются цифровым представлением взаимозаменяемых финансовых продуктов. Кроме того, они являются цифровым представлением взаимозаменяемых нефинансовых продуктов, будучи как твердыми активами, т. е. осязаемыми и физическими, так и мягкими, т. е. нематериальными или цифровыми товарами. В этом смысле возможности практически безграничны, и есть мнение, что метавселенная представляет собой следующее поколение Интернета (Pooyandeh et al., 2022). Так или иначе, метавселенная, по-видимому, является, по крайней мере, развитием Интернета с преобладающим акцентом на социальное взаимодействие. По мере развития метавселенной и увеличения числа пользователей все больше личной информации, включая нейронную, будет подвергаться риску, как мы увидим в следующих разделах (Pooyandeh et al., 2022).

3.3. Цифровое сенсорное взаимодействие в метавселенной

В настоящее время, помимо взаимодействия с экраном смартфона, планшета или другого устройства посредством прикосновения, сенсорное взаимодействие с цифровой средой обычно ограничивается слухом и зрением, т. е. в общей сложности тремя из пяти традиционно известных органов чувств человека. Похоже, что в ближайшем будущем взаимодействие может включать в себя более базовые органы чувств, и их восприятие будет все больше походить на восприятие физического мира. В 2013 г. Google опубликовала поисковую систему Google Nose, которая позволяет находить нужный объект с помощью обоняния[54]. Хотя этот сервис был создан как своего рода первоапрельская шутка и для конкретных условий того времени, он был признан успешным. В то же время стало ясно, что пользователи готовы вывести взаимодействие с Интернетом на новый уровень[55]. С тех пор были разработаны удобные для пользователя цифровые сенсорные системы, позволяющие включить обоняние в сферу обычного взаимодействия с цифровой средой. Например, пользователи цифровой среды могут понюхать духи, прежде чем приобрести их в Сети. Цель состоит в том, чтобы пользователи, выйдя из дома,

---

53 Simões Ferreira, R. (2022, Desember 29). With holograms or in the metaverse, how digital has already reinvented 'live'. Jornal de Notícias. https://clck.ru/3Nkqum

54 См. веб-сайт компании Google Nose Beta: https://clck.ru/3Nkqw4

55 Nordyke, K. (2023). Google's April Fools' Joke: Search and Smell (Video). The Hollywood Reporter. https://goo.su/UBRW9

могли вдохнуть запах моря, как будто они находятся на пляже, или даже ощутить влагу на своей коже. То же самое касается вкуса и ощущения аромата. В 2020 г. в Университете Мэйдзи в Японии был разработан прототип (получивший название «Дегустатор»), который позволяет пользователю ощутить различные вкусы с помощью устройства, адаптированного для прикосновения языком[56]. В этом смысле в контексте сенсорного взаимодействия пользователей с цифровой средой все чаще используются понятия «дополненный человек» или «дополненный человеческий интеллект».

В рамках метавселенной мобильные и носимые устройства, такие как, например, гарнитуры виртуальной и/или дополненной реальности, кроме датчиков, позволяющих пользователю обнаруживать движение или звук, могут также включать в себя датчики других типов. В частности, системы виртуальной реальности состоят из инерциальных измерительных устройств и включают акселерометры, гироскопы и магнитометры. Также существуют датчики времени, дыхания и освещенности. Системы дополненной реальности определяют местоположение пользователя и то, что он видит или слышит. Большинство гарнитур оснащены датчиками времени полета (time-of-flight, ToF), поверхностно-излучающими лазерами с вертикальным резонатором (vertical cavity surface-emitting laser, VCSEL), бинокулярными датчиками глубины и оптическими датчиками для изучения структур. Обе системы могут также работать с датчиками звука, такими как направленные микрофоны, а также с тепловыми датчиками, сенсорными датчиками, передними и задними видеокамерами. Сенсорные датчики используются для обмена информацией между людьми и машинами в форме человеко-машинного интерфейса, при этом активируется тактильный стимул (как, например, в сенсорной панели). Большинство из этих датчиков используются в интернете вещей в промышленности, медицине, в беспилотных летательных аппаратах и человекоподобных роботах (Pooyandeh et al., 2022).

Однако устройства для деятельности в метавселенной, которые в настоящее время массово выпускаются на рынок, по-прежнему имеют множество ограничений (с точки зрения как аппаратного, так и программного обеспечения). Подавляющее большинство из них еще недостаточно развиты, чтобы обеспечить полное погружение в метавселенную. Восприятие ощущений в физическом мире по-прежнему более совершенно, чем в цифровом. Следовательно, подавляющее большинство платформ метавселенной не справляются с большими объемами пользовательских данных, что, в свою очередь, означает, что мы также не близки к массовому внедрению таких устройств. Лучшим примером этого является очевидный провал гарнитуры Apple Vision Pro, которая была призвана заменить клавиатуру, сенсорный экран и компьютерную мышь[57]. В этом контексте в литературе (как мы увидим в следующем разделе) ИМК признается ключевой технологией для достижения полной интеграции между пользователем и метавселенной в среднесрочной и долгосрочной

[56] Grad, P. (2020). Digital device serves up a taste of virtual food. TechXplore. https://clck.ru/3Nkr7r

[57] Mitchell, A. (2024, November 12). Apple's Vision Pro flop: Company scales back production of $3,500 VR headset amid lackluster sales, customer complaints. New York Post. https://clck.ru/3Nm5Ka

перспективе (Bernal et al., 2022)[58]. Кроме того, массовому внедрению этой новой модели сенсорного взаимодействия с Интернетом способствует разработка передовых датчиков и аппаратного обеспечения, а также других видов оборудования, связанных с метавселенной[59].

3.4. Интерфейс «мозг – компьютер» в метавселенной

Нанотехнологическая компания Neuralink Corp.[60], принадлежащая, в частности, Илону Маску[61], разработала тип ИМК, который требует нейрохирургической операции для имплантации интегральной схемы (чипа) в мозг пользователя. Это одновременно интригует и обескураживает многих потенциальных потребителей. Этот тип ИМК позволяет установить двунаправленное взаимодействие с мозгом, которое включает в себя как нейронные механизмы обучения и памяти, так и нейростимуляцию. В целом, хотя эти устройства можно использовать для восстановления способности говорить, писать и даже ходить, к ним все равно относятся с некоторым подозрением[62]. Тем не менее ученые рассматривают и обсуждают современное состояние данной проблемы, в частности, путем сравнения текущего ИМК с определенными устройствами виртуальной и/или дополненной реальности, которые представляют собой своего рода шлем с функцией снятия ЭЭГ. Было обнаружено, что проблемы с эргономикой затрудняют развитие гарнитур виртуальной и/или дополненной реальности, которые содержат слишком много датчиков ЭЭГ для мониторинга областей мозга. Считается, что гарнитуры виртуальной и/или дополненной реальности, которые смягчают воздействие шума, возникающего в результате обработки мозговых волн, по-видимому, лучше всего подходят для встраивания датчиков ЭЭГ (Orlosky et al., 2021). Также утверждают, что сочетание ресурсов и технологий, включая виртуальную и/или дополненную реальность, цифровые аватары, системы сенсорного взаимодействия и ИМК, способствует широкому внедрению метавселенных во все сферы повседневной жизни. Если это так, то это могло бы

---

58 Следовательно, осознаем мы это или нет, но в настоящее время мы являемся свидетелями быстрой и радикальной трансформации области делового и коммерческого этикета как с точки зрения продуктов и методов производства, так и с точки зрения видов услуг и способов их предоставления. Например, подсознание или сны пользователей, по-видимому, не защищены от маркетинговых кампаний или даже пропаганды. Существуют системы сенсорного взаимодействия, которые могут влиять на содержание снов пользователя с помощью стимулов, воздействующих на мозг до или во время сна. В частности, они побуждают пользователя увидеть определенный продукт или услугу во сне.

59 Genser, J., Damianos, S., & Yuste, R. (2024). Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies. The Neurorights Foundation. https://clck.ru/3NkrK7

60 Устройство ИМК, разработанное компанией Neuralink, состоит из небольшого зонда с более чем тремя тысячами электродов, соединенных гибкими проводами тоньше человеческого волоса. Это устройство может отслеживать активность 1000 нейронов головного мозга. Также создан «нейрохирургический робот», который может вводить в мозг 192 электрода в минуту. См. Galeon, D. (2017, November 22). Experts: Artificial Intelligence Could Hijack Brain-Computer Interfaces. Can we prevent AI from hacking into the human brain? Futurism. https://clck.ru/3NkrMh

61 См. веб-сайт компании Neuralink. https://clck.ru/3NkrP3

62 Hall, S. B., & Baier-Lentz, M. (2022, Februry 7). 3 technologies that will shape the future of the metaverse – and the human experience. The World Economic Forum. https://clck.ru/3NkrRf

изменить социальный опыт восприятия пространства и времени. Сочетание метавселенной и ИМК является аргументом в пользу создания новых форм социального взаимодействия и интероперабельности, что делает коммуникацию между физическим и цифровым миром еще более быстрой, эффективной и действенной, а также более прозрачной (Dwivedi et al., 2022). В дополнение к своей полезности в медицинском контексте, комбинация метавселенной и ИМК также найдет применение в других контекстах. В частности, это позволит пользователям управлять определенными объектами (материальными или нематериальными, такими как продукты робототехники или цифровые аватары), или просто наслаждаться видеоиграми или другими развлечениями с помощью своего разума, мысленного проговаривания, аутентификации с помощью мозговых волн (Bernal et al., 2022). Это сочетание также может быть использовано для когнитивной оценки, эмоционального контроля и повышения когнитивной работоспособности. В современной литературе также исследуется возможность использования ИМК для обеспечения прямой связи между мозгом разных испытуемых, используя как нейронные механизмы обучения и запоминания, так и нейростимуляцию (Bernal et al., 2022). Однако, несмотря на известную эволюцию ИМК за последние несколько десятилетий, их полная реализация в сценариях метавселенной еще не изучена так глубоко, как она того заслуживает. Некоторые проблемы все еще остаются нерешенными. Во-первых, нужно провести широкий анализ того, какой вклад ИМК могут внести в развитие метавселенной. Во-вторых, представляется необходимым измерить производительность этих систем и определить тенденции и проблемы, с которыми сталкивается ИМК при применении в сценарии метавселенной. И последнее, но не менее важное: необходимо определить проблемы, ограничения и риски, связанные с использованием ИМК в метавселенной (Bernal et al., 2022).

3.5. Нейрохакинг в метавселенной

Между Интернетом и метавселенной много общего, когда речь заходит о проблемах кибербезопасности, среди которых взлом учетных записей, фишинг, вредоносное ПО и т. д. Несмотря на различия в инфраструктуре, метавселенная (Web 3.0 и Web 4.0) представляет новые виды киберпреступлений, которые отличаются от тех, что совершаются на традиционных веб-сайтах (Web 2.0). По мере расширения использования криптоактивов и цифровых валют центральных банков хакеры будут проявлять все больший интерес к взлому метавселенной (Pooyandeh et al., 2022). В этом смысле мониторинг метавселенной и обнаружение атак на новых платформах более сложны, чем на традиционных платформах. Как было показано в предыдущих разделах, с коммерциализацией и массовым внедрением продуктов, связанных с метавселенной и виртуальными мирами, масштабы деятельности хакеров существенно возрастут. Среди основных связанных с этим рисков – появление «иммерсивных атак». Это новый тип атаки в виртуальной среде, который состоит в злонамеренном манипулировании устройством с целью нанесения физического или психического вреда пользователю или причинения ему неудобств. Также заслуживает внимания атака «человек – джойстик». Она заключается в управлении пользователями, погруженными в системы виртуальной и/или дополненной реальности в метавселенной, без их ведома или разрешения, с целью перемещения их физического тела в другое место в физическом мире. При использовании комбинации ИМК, особенно тех,

которые используются для нейростимуляции, атаки направляются на чрезмерную стимуляцию или подавление определенных областей мозга, тем самым нарушая нормальную мозговую деятельность. Ущерб, причиняемый такого рода действиями, по-видимому, способен даже воссоздать последствия нейродегенеративных заболеваний, хотя в этом отношении еще предстоит провести дополнительные исследования (Bernal et al., 2022)[63].

3.6. Интерфейс «мозг – компьютер» на основе искусственного интеллекта

Искусственный интеллект способствовал прогрессу в анализе и расшифровке нейронной активности, а также развитию сектора ИМК. За последнее десятилетие появилось множество приложений для ИМК с использованием ИИ или даже исключительно на его основе. Эти «умные» ИМК, в том числе двигательные и сенсорные, показали значительный успех в области медицины. Помимо улучшения качества жизни пациентов, они расширили спортивные возможности обычных людей и ускорили эволюцию роботов и достижений нейрофизиологии. Однако, несмотря на технический прогресс, все еще существует ряд проблем, связанных с длительностью машинного обучения, получением результатов в режиме реального времени, а также измерением и регистрацией мозговой активности в рамках работы этого нового типа ИМК. Как было показано в предыдущем разделе (и в целом в гл. III), все еще существует необходимость в дополнительных исследованиях в этом направлении (Zhang et al., 2020).

3.7. Нейрохакинг и искусственный интеллект

Хотя нет достаточных доказательств того, что современные хакерские группы обладают большим техническим опытом в управлении IoT-системами на основе искусственного интеллекта, они, по всей вероятности, уже реализуют свой огромный потенциал. Большинство из этих преступных организаций состоят из хакеров, которые умеют манипулировать любыми компьютерными системами и эксплуатировать их в злонамеренных целях. Не стоит забывать, что атаки проводятся 24 часа в сутки и из любой точки мира (Velasco, 2022). С появлением технологий ИМК, основанных на искусственном интеллекте, киберпреступники, похоже, нашли новое средство для усиления своей незаконной деятельности и, в частности, новые возможности для разработки и осуществления атак на отдельных лиц, компании и даже правительства. В литературе выдвигается множество гипотез на этот счет. Во-первых, если хакер возьмет под контроль ИМК, подключенные к большому количеству людей, он сможет манипулировать ими, заставляя проголосовать за конкретного кандидата, конкретную партию или по конкретному вопросу, тем самым тайно подчиняя себе правительство и/или всю инфраструктуру государства. На данный момент это кажется в высшей степени невероятным сценарием, но не исключен риск того, что определенные хакерские группы превратят устройства ИМК в своего рода армию

[63] Стоит отметить, что и Интерпол, и Европол осведомлены о преступной деятельности, осуществляемой в метавселенной. В этой связи см. Interpol. (2022, October 20). Interpol launches first global police Metaverse. https://clck.ru/3NkriG; Europol. (2022, October 21). Policing in the metaverse: what law enforcement needs to know. https://clck.ru/3Nkrnf

программируемых роботов, готовых выполнять все команды «хозяина»[64]. Хотя ИМК были разработаны людьми для взлома человеческого мозга, существует риск того, что ИМК будет использован с той же целью искусственным интеллектом[65]. Вероятно, некоторые системы искусственного интеллекта сами могут превратиться в хакеров, как только станут «разумными» (Esmaeilzadeh & Vaezi, 2021)[66, 67]. Если это так, то все указывает на то, что в их распоряжении будут компьютеризированные средства для оценки уязвимостей любых социальных, экономических и политических систем, а затем их использования с беспрецедентной скоростью, масштабом и размахом, способами, невообразимыми для ограниченного человеческого разума. Это не просто разница в уровне интеллекта – это борьба между видами. Может даже случиться так, что некоторые системы искусственного интеллекта будут пытаться взломать другие системы искусственного интеллекта, а люди останутся лишь наблюдателями и их риски будут составлять не более чем сопутствующий ущерб. Все указывает на то, что этот сценарий не является преувеличением. На самом деле ни одна из этих гипотез не требует создания научно-фантастической технологии далекого будущего. Вовсе не кажется неразумным утверждать, что развитие искусственного интеллекта станет настолько стремительным, что даже превзойдет человеческое понимание, как, по сути, уже, кажется, и просходит[68].

Заключение

Цель нашего исследования – внести свой вклад в изучение нейрохакинга в эпоху цифровых технологий и искусственного интеллекта и, прежде всего, повысить осведомленность о последствиях для нейробезопасности (а также этических последствиях), возникающих в результате злонамеренного использования технологий нейроманипулирования, связанных с метавселенной и искусственным интеллектом.

В результате было установлено, что возможные выгоды от разработки, массового внедрения и коммерциализации такого рода технологий могут быть неадекватными возможным рискам. Как и любой компьютер, компьютерная сеть или большинство других форм информационно-коммуникационных технологий, аппаратное ядро основано на электронных компонентах, способных обрабатывать данные, т. е. записывать, обрабатывать и хранить данные (и информацию), а также выполнять алгоритмы. Таким образом, подавляющее большинство из них, в принципе, можно взломать. Стремительный технологический прогресс не является сдерживающим фактором этих процессов. Напротив, в конечном итоге он способствует им или становится вызовом. Вспомним о недавнем росте кибератак на общественные

---

64 Lau, J. (2020, November 18). Hacking Humans: How Neuralink May Give AI The Keys To Our Brains. Forbes. https://clck.ru/3NkrqV

65 Schneier, B. (2021). The Coming AI Hackers. Belfer Center for Science and International Affairs. Harvard Kennedy School. https://clck.ru/3NkrrW

66 Там же.

67 См. также Johnson, A. (2024, March 19). Consciousness for Artificial Intelligence? IEEE Pulse. https://clck.ru/3Nkrtg

68 Schneier, B. (2021). The Coming AI Hackers. Belfer Center for Science and International Affairs. Harvard Kennedy School. https://clck.ru/3Nkrw7

организации или росте киберпреступности в целом. В настоящее время мы наблюдаем серьезные последствия с точки зрения финансового и зачастую репутационного ущерба. Однако в ближайшем будущем, в мире «мультивселенной», состоящей из метавселенных с «умными технологиями», мы столкнемся с такими последствиями внедрения чипов в человеческий мозг для установления своего рода симбиоза с Интернетом и искусственным интеллектом, какие не в состоянии даже вообразить. Уже сегодня каждый аспект человеческой жизни отслеживается[69] и анализируется[70] мобильными устройствами (такими как смартфоны и/или умные часы), данные собираются и хранятся с целью создания подробных психографических профилей, но человеческий мозг содержит информацию, которая по самой своей природе не может быть записана без нейронного взаимодействия. Установление прямого соединения между человеческим мозгом, мобильными устройствами и искусственным интеллектом может открыть доступ к человеческому сознанию. Это также может позволить определенным группам хакеров (которые обычно на шаг опережают протоколы безопасности) взять под контроль человеческий разум, включая процесс принятия решений и их исполнение. В этом случае представьте себе последствия для процедур голосования и в контексте политических выборов или других более или менее мирных политических движений. Представьте себе неограниченные возможности для создания «суперсолдат» в условиях войн и даже для наблюдения и общественного контроля. Представьте себе в предельном и апокалиптическом сценарии будущего возможность того, что сам искусственный интеллект сможет взять под контроль нейронный интерфейс и, таким образом, человеческое сознание.

В любом случае похоже, что в ближайшем будущем будет становиться все легче внедрять идеи и даже идеологии в сознание людей (что в настоящее время происходит в основном через социальные сети). В какой степени можно будет гарантировать защиту персональных данных в случае нейроатаки? В этом контексте термин «персональные данные» приобретает совершенно новый смысл. Учитывая фрейдистскую теорию системы «восприятие – сознание», в какой степени можно гарантировать защиту самого «сознательного психического процесса», включая предыдущее бессознательное состояние? Вспомним фильм 2010 г. «Начало» с Леонардо Ди Каприо в главной роли. В этом контексте возникает также ряд философских вопросов. Что такое реальный мир? Как мы можем узнать, реален он или нет? Можно ли считать жизнь в метавселенной «более реальной», чем то, что считается реальной жизнью сегодня?

Среди самых известных предупреждений Илона Маска (которого часто считают своего рода спасителем человечества[71]) выделяются два весьма необычных. В 2018 г. он заявил, что искусственный интеллект может стать «бессмертным диктатором»[72], от которого человечество «никогда не сможет убежать». В 2020 г.

---

69 Szoldra, P. (2016, September 16). This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks. Business Insider. https://clck.ru/3Nkry8

70 Shane, S., Rosenberg, M., & Lehren, A. (2017, March 7). WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents. The New York Times. https://clck.ru/3Nkrzw

71 Dowd, M. (2017, March 26). Elon Musk's Billion-Dollar Crusade to Stop the A.I. Apocalypse. The Vanity Fair. https://clck.ru/3NkkHp

72 Holley, P. (2018, April 6). Elon Musk's nightmarish warning: AI could become 'an immortal dictator from which we would never escape'. The Washington Post. https://clck.ru/3NkkGv

он снова предупредил о той же проблеме, на этот раз заявив, что «искусственный интеллект обгонит человека менее чем за пять лет»[73]. Однако? помимо этих, мягко говоря, интригующих высказываний, Илон Маск также постоянно, упорно и без видимых ограничений стремится развивать функциональность и технологические возможности этого типа технологий, а также расширять возможные формы их применения. Впечатляют современные технологические разработки в области робототехники, созданные компанией Tesla, Inc. В частности, стоит упомянуть проект Tesla Optimus[74] и создание человекоподобных роботов по прозвищу Оптимус[75], внешний вид и характеристики которых напоминают роботов из фильма 2004 г. «Я, робот» с Уиллом Смитом в главной роли или роботов Skynet из фильма «Терминатор» 1995 г. с Арнольдом Шварценеггером. Не открываем ли мы неосознанно двери в вымышленный, мрачный мир, как в фильме «Матрица», снятом в далеком 1999 г.? Только время покажет.

Список литературы

Abegão Alves, C. (2020). Contra a mente: ensaio de integração das lesões resultantes de intervenções na mente no artigo 143.º do Código Penal. In M. Fernanda Palma et al. (org.). *Livro em Memória do Professor Doutor João Curado Neves. Associação Académica da Faculdade de Direito de Lisboa* (pp. 215–235). AAFDL Editora. (In Portug.).

Bernal, S. L., Pérez, M. Q., Martínez Beltrán, E. T., Martínez Pérez, G., & Huertas Celdrán, A. (2022). When Brain-Computer Interfaces Meet the Metaverse: Landscape, Demonstrator, Trends, Challenges, and Concerns. *Computer Science – Human-Computer Interaction*. https://doi.org/10.48550/arXiv.2212.03169

Bublitz, J. C., & Merkel, R. (2014). Crimes Against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination. *Criminal Law and Philosophy*, *8*, 51–77. https://doi.org/10.1007/s11572-012-9172-y

Czech, A. (2021). Brain-Computer Interface Use to Control Military Weapons and Tools. In S. Paszkiel (Ed.), *Control, Computer Engineering and Neuroscience. ICBCI 2021. Advances in Intelligent Systems and Computing* (Vol. 1362). Springer, Cham. https://doi.org/10.1007/978-3-030-72254-8_20

Denning, T., Matsuoka, Y., & Kohno, T. (2009). Neurosecurity: Security and privacy for neural devices. *Neurosurgical Focus*, *27*(1), E7. https://doi.org/10.3171/2009.4.focus0985

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, Bh., Buhalis, D., Cheung, Ch. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, Ch., Jebabli, I., Janssen, … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Ford, M. (2016). *Robôs: A Ameaça de um futuro sem emprego*. Bertrand Editora. (In Portug.).

Esmaeilzadeh, H., & Vaezi, R. (2021). Conscious AI. *arXiv:2105.07879*. https://doi.org/10.48550/arXiv.2105.07879

Ienca, M., & Haselager, P. (2016). Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity. *Ethics and Information Technology*, *18*, 117–129. https://doi.org/10.1007/s10676-016-9398-9

Kotchetkov, I., Hwang, B. Y., Appelboom, G., Kellner, Ch. P., & Connolly E. S. Jr. (2010). Brain-computer interfaces: Military, neurosurgical, and ethical perspective. *Neurosurgical Focus*, *28*(5), E25. https://doi.org/10.3171/2010.2.focus1027

[73] Cuthbertson, A. (2020, July 27). Elon Musk claims AI will overtake humans 'in less than five years'. Independent. https://clck.ru/3NkkF2

[74] Levin, T. (2022, January 27). Elon Musk says Tesla's humanoid robot is the most important product it's working on – and could eventually outgrow its car business. Business Insider. https://clck.ru/3NkkDD

[75] Gomez, B. (2021, August 24). Elon Musk warned of a 'Terminator'-like AI apocalypse – now he's building a Tesla robot. CNBC. https://clck.ru/3NkkBk

Li, Q., Ding, D., & Conti, M. (2015). Brain-computer interface applications: Security and privacy challenges. *IEEE conference on communications and network security (CNS). Florence, 2015* (pp. 663–666). https://doi.org/10.1109/CNS.2015.7346884

Marques, G., & Martins, L. (2006). *Direito da informática* (2.ª Edição). Almedina. (In Portug.).

Miranda, R., Casebeer, W. D., Hein, A. M., Judy, J. W., Krotkov, E. P., Laabs, T. L., Manzo, J. E., Pankratz, K. G., Pratt, G. A., Sanchez, J. C., Weber, D. J., Wheeler, T. L., & Ling, G. S. F. (2015). DARPA-funded efforts in the development of novel brain-computer interface technologies. *Journal of Neuroscience Methods*, *244*, 52–67. https://doi.org/10.1016/j.jneumeth.2014.07.019.

Mochan, A., Parkin, B., Farinha, J., & Bailey, G. (2025). *Emerging applications of neurotechnology and their implications for EU governance*. Publications Office of the European Union. Luxembourg.

Moulin, T. (2022). 'I Will Control Your Mind': The International Regulation of Brain-Hacking. *San Diego International Law Journal*, *24*(65).

Orlosky, J., Sra, M., Bektaş, K., Peng, H., Kim, J., Kosmyna, N., Höllerer, T., Steed, A., Kiyokawa, K., Akşit, K. (2021). Telelife: The Future of Remote Living. *Frontiers in Virtual Reality*, *2*, 763340. https://doi.org/10.3389/frvir.2021.763340

Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-Based Metaverse: A Survey. *Applied Sciences. MDPI*, *12*(24), 12993. https://doi.org/10.3390/app122412993

Radu, R. (2024). Neurotechnologies and the future of internet governance. Technical Report. EUI. RSC (Global Governance Programme). *GIFI. Issue Brief*.

Rodrigues, B. S. (2009). *Direito Penal Especial. Direito Penal Informático-Digital*. Almedina. (In Portug.).

Rosenfeld, P., Biroschak, J., & Furedy, J. (2006). P300-based detection of concealed autobiographical versus incidentally acquired information in target and non-target paradigms. *International Journal of Psychophysiology*, *60*(3), 251–259. https://doi.org/10.1016/j.ijpsycho.2005.06.002

Rosenfeld, P. (2011). P300 in detecting concealed information. In B. Verschuere, G. Ben-Shakhar, & E. Meijer (Eds), *Memory detection: Theory and application of the concealed information test* (pp. 63–89). Cambridge University Press. https://doi.org/10.1017/CBO9780511975196.005

Shen, F. (2013). Mind, Body, and the Criminal Law. *Minnesota Law Review*, *97*, 2036–2175.

Vallabhaneni, A., Wang, T., & He, B. (2005). Brain – Computer Interface. In B. He (Ed.), *Neural Engineering. Bioelectric Engineering* (pp. 85–121). Springer. Boston, MA. https://doi.org/10.1007/0-306-48610-5_3

Van Gerven, M., Farquhar, J., Schaefer, R., Vlek, R., Geuze, J., Nijholt, A., Ramsey, N., Haselager, P., Vuurpijl, L., Gielen, S., & Desain, P. (2009). The brain-computer interface cycle. *Journal of Neural Engineering*, *6*(4), 041001. https://doi.org/10.1088/1741-2560/6/4/041001

Vasconcelos Casimiro, S. (2000). *A responsabilidade civil pelo conteúdo da informação transmitida pela Internet*. Almedina. (In Portug.).

Velasco, C. (2022). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, *23*, 109–126. https://doi.org/10.1007/s12027-022-00702-z

Venâncio, P. (2011). *Lei do Cibercrime. Anotada e Comentada*. Almedina. (In Portug.).

Yuan, B., Hsieh, Chih-Hung, & Chang, Chien-Ching (2010). National technology foresight research: A literature review from 1984 to 2005. *International Journal of Foresight and Innovation Policy*, *6*(1), 5–35. http://dx.doi.org/10.1504/IJFIP.2010.032663

Zhang, X., Ma, Z., Zheng, H., Li, T., Chen, K., Wang, X., Liu, Ch., Xu, L., Wu, X., Lin, D., Lin, H. (2020). The combination of brain-computer interfaces and artificial intelligence: applications and challenges. *Annals of Translational Medicine*, *8*(11), PMC7327323. https://doi.org/10.21037/atm.2019.11.109

Сведения об авторе

Коэльо Диого Перейра – аспирант, Севильский университет
Адрес: Испания, 41013, г. Севилья, Калле Сан Фернандо, д. 4
E-mail: diopercoe@alum.us.es
ORCID ID: https://orcid.org/0000-0002-2082-1231
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57703490300
WoS Researcher ID: https://www.webofscience.com/wos/author/record/GLU-8923-2022
Google Scholar ID: https://scholar.google.com/citations?user=-laUdL8AAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

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

История статьи

Дата поступления – 5 мая 2025 г.
Дата одобрения после рецензирования – 26 мая 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.

Research article
UDC 34:004:343.721:004.8
EDN: https://elibrary.ru/smgmxq
DOI: https://doi.org/10.21202/jdtl.2025.16

Neurohacking in the Digital and Artificial Intelligence Age: Legal Aspects of Protecting Neural Information

Diogo Pereira Coelho
University of Seville, Seville, Spain

Keywords

artificial intelligence,
brain-computer interface,
cybercrime,
digital technologies,
law,
metaverse,
neurocrime,
neurohacking,
neurosecurity,
neurotechnologies

Abstract

Objective: to contribute to the concept of neurocrime; to study the current and future risks from the viewpoint of cybersecurity in the context of digitalization and artificial intelligence development.

Methods: the study uses a critical and descriptive analysis of the relationship between cybercrime and neurocrime. It provides a conceptual distinction between the brain-computer interface and its use and describes the differences between neural and mental manipulation. The legal autonomy of crimes against mental integrity in relation to crimes against physical integrity is investigated. The methodological framework includes the analysis of existing prototypes of neurocrimes based on a four-phase brain-computer interface cycle and the study of the features of neurohacking in the context of the metaverse and artificial intelligence technologies.

Results: the study revealed the essential characteristics of neurohacking as the misuse of neural devices to gain unauthorized access to and manipulate neural information. Four main types of brain-computer interface applications subject to neurohacking are identified: neuromedical applications, user authentication systems, video games, and smartphone-based applications. The modalities of neurohacking were established at each phase of the brain-computer interface cycle: manipulations at the stage of neural information input, measuring and recording of brain activity, decoding and classifying neural information, as well as at the stage of the result output. The specific threats of neurohacking in the era of digitalization are analyzed, including immersive attacks and human joystick attacks in the metaverse.

© Coelho D. P., 2025

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Scientific novelty: for the first time, a comprehensive differentiation of the concepts of neurocrime and cybercrime was carried out, highlighting their specific legal consequences. The author proposed a classification of neurocrimes based on the four-phase cycle of the brain-computer interface. The study substantiated the need to distinguish mental integrity as an independent object of legal protection, different from the protection of physical integrity. For the first time, the features of neurohacking in the context of the metaverse and artificial intelligence technologies were investigated, including the analysis of new types of attacks and threats to neurosecurity.

Practical significance: the study results are important for the development of legal regulation in the field of cybersecurity and the corresponding regulations. The identified types of neurocrimes and their classification can help to create a specialized legislation on the protection of neural data and mental integrity. Practical recommendations on ensuring the neurosecurity of brain-computer interfaces are in demand in medical practice, video game industry, authentication systems, and for the development of smartphone applications.

For citation

Coelho, D. P. (2025). Neurohacking in the Digital and Artificial Intelligence Age: Legal Aspects of Protecting Neural Information. *Journal of Digital Technologies and Law, 3*(3), 397–430. https://doi.org/10.21202/jdtl.2025.16

References

Abegão Alves, C. (2020). Contra a mente: ensaio de integração das lesões resultantes de intervenções na mente no artigo 143.º do Código Penal. In M. Fernanda Palma et al. (org.). *Livro em Memória do Professor Doutor João Curado Neves. Associação Académica da Faculdade de Direito de Lisboa* (pp. 215–235). AAFDL Editora. (In Portug.).

Bernal, S. L., Pérez, M. Q., Martínez Beltrán, E. T., Martínez Pérez, G., & Huertas Celdrán, A. (2022). When Brain-Computer Interfaces Meet the Metaverse: Landscape, Demonstrator, Trends, Challenges, and Concerns. *Computer Science – Human-Computer Interaction*. https://doi.org/10.48550/arXiv.2212.03169

Bublitz, J. C., & Merkel, R. (2014). Crimes Against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination. *Criminal Law and Philosophy*, *8*, 51–77. https://doi.org/10.1007/s11572-012-9172-y

Czech, A. (2021). Brain-Computer Interface Use to Control Military Weapons and Tools. In S. Paszkiel (Ed.), *Control, Computer Engineering and Neuroscience. ICBCI 2021. Advances in Intelligent Systems and Computing* (Vol. 1362). Springer, Cham. https://doi.org/10.1007/978-3-030-72254-8_20

Denning, T., Matsuoka, Y., & Kohno, T. (2009). Neurosecurity: Security and privacy for neural devices. *Neurosurgical Focus*, *27*(1), E7. https://doi.org/10.3171/2009.4.focus0985

Dias Venâncio, P. (2011). *Lei do Cibercrime. Anotada e Comentada*. Almedina. (In Portug.).

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, Bh., Buhalis, D., Cheung, Ch. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, Ch., Jebabli, I., Janssen, … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Ford, M. (2016). *Robôs: A Ameaça de um futuro sem emprego*. Bertrand Editora. (In Portug.).

Esmaeilzadeh, H., & Vaezi, R. (2021). Conscious AI. *arXiv:2105.07879*. https://doi.org/10.48550/arXiv.2105.07879

Ienca, M., & Haselager, P. (2016). Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity. *Ethics and Information Technology*, *18*, 117–129. https://doi.org/10.1007/s10676-016-9398-9

Kotchetkov, I., Hwang, B. Y., Appelboom, G., Kellner, Ch. P., & Connolly E. S. Jr. (2010). Brain-computer interfaces: Military, neurosurgical, and ethical perspective. *Neurosurgical Focus*, *28*(5), E25. https://doi.org/10.3171/2010.2.focus1027

Li, Q., Ding, D., & Conti, M. (2015). Brain-computer interface applications: Security and privacy challenges. *IEEE conference on communications and network security (CNS). Florence, 2015* (pp. 663–666). https://doi.org/10.1109/CNS.2015.7346884

Marques, G., & Martins, L. (2006). *Direito da informática* (2.ª Edição). Almedina. (In Portug.).

Miranda, R., Casebeer, W. D., Hein, A. M., Judy, J. W., Krotkov, E. P., Laabs, T. L., Manzo, J. E., Pankratz, K. G., Pratt, G. A., Sanchez, J. C., Weber, D. J., Wheeler, T. L., & Ling, G. S. F. (2015). DARPA-funded efforts in the development of novel brain-computer interface technologies. *Journal of Neuroscience Methods*, *244*, 52–67. https://doi.org/10.1016/j.jneumeth.2014.07.019.

Mochan, A., Parkin, B., Farinha, J., & Bailey, G. (2025). *Emerging applications of neurotechnology and their implications for EU governance*. Publications Office of the European Union. Luxembourg.

Moulin, T. (2022). 'I Will Control Your Mind': The International Regulation of Brain-Hacking. *San Diego International Law Journal*, *24*(65).

Orlosky, J., Sra, M., Bektaş, K., Peng, H., Kim, J., Kosmyna, N., Höllerer, T., Steed, A., Kiyokawa, K., Akşit, K. (2021). Telelife: The Future of Remote Living. *Frontiers in Virtual Reality*, *2*, 763340. https://doi.org/10.3389/frvir.2021.763340

Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-Based Metaverse: A Survey. *Applied Sciences. MDPI*, *12*(24), 12993. https://doi.org/10.3390/app122412993

Radu, R. (2024). Neurotechnologies and the future of internet governance. Technical Report. EUI. RSC (Global Governance Programme). *GIFI. Issue Brief*.

Rodrigues, B. S. (2009). *Direito Penal Especial. Direito Penal Informático-Digital*. Almedina. (In Portug.).

Rosenfeld, P., Biroschak, J., & Furedy, J. (2006). P300-based detection of concealed autobiographical versus incidentally acquired information in target and non-target paradigms. *International Journal of Psychophysiology*, *60*(3), 251–259. https://doi.org/10.1016/j.ijpsycho.2005.06.002

Rosenfeld, P. (2011). P300 in detecting concealed information. In B. Verschuere, G. Ben-Shakhar, & E. Meijer (Eds), *Memory detection: Theory and application of the concealed information test* (pp. 63–89). Cambridge University Press. https://doi.org/10.1017/CBO9780511975196.005

Shen, F. (2013). Mind, Body, and the Criminal Law. *Minnesota Law Review*, *97*, 2036–2175.

Vallabhaneni, A., Wang, T., & He, B. (2005). Brain – Computer Interface. In B. He (Ed.), *Neural Engineering. Bioelectric Engineering* (pp. 85–121). Springer. Boston, MA. https://doi.org/10.1007/0-306-48610-5_3

Van Gerven, M., Farquhar, J., Schaefer, R., Vlek, R., Geuze, J., Nijholt, A., Ramsey, N., Haselager, P., Vuurpijl, L., Gielen, S., & Desain, P. (2009). The brain-computer interface cycle. *Journal of Neural Engineering*, *6*(4), 041001. https://doi.org/10.1088/1741-2560/6/4/041001

Vasconcelos Casimiro, S. (2000). *A responsabilidade civil pelo conteúdo da informação transmitida pela Internet*. Almedina. (In Portug.).

Velasco, C. (2022). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, *23*, 109–126. https://doi.org/10.1007/s12027-022-00702-z

Yuan, B., Hsieh, Chih-Hung, & Chang, Chien-Ching (2010). National technology foresight research: A literature review from 1984 to 2005. *International Journal of Foresight and Innovation Policy*, *6*(1), 5–35. http://dx.doi.org/10.1504/IJFIP.2010.032663

Zhang, X., Ma, Z., Zheng, H., Li, T., Chen, K., Wang, X., Liu, Ch., Xu, L., Wu, X., Lin, D., Lin, H. (2020). The combination of brain-computer interfaces and artificial intelligence: applications and challenges. *Annals of Translational Medicine*, *8*(11), PMC7327323. https://doi.org/10.21037/atm.2019.11.109

Author information

Diogo P. Coelho – PhD student, University of Seville
Address: 4 Calle San Fernando, 41013 Sevilla, Spain
E-mail: diopercoe@alum.us.es
ORCID ID: https://orcid.org/0000-0002-2082-1231
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57703490300
WoS Researcher ID: https://www.webofscience.com/wos/author/record/GLU-8923-2022
Google Scholar ID: https://scholar.google.com/citations?user=-laUdL8AAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – May 5, 2025
Date of approval – May 26, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025