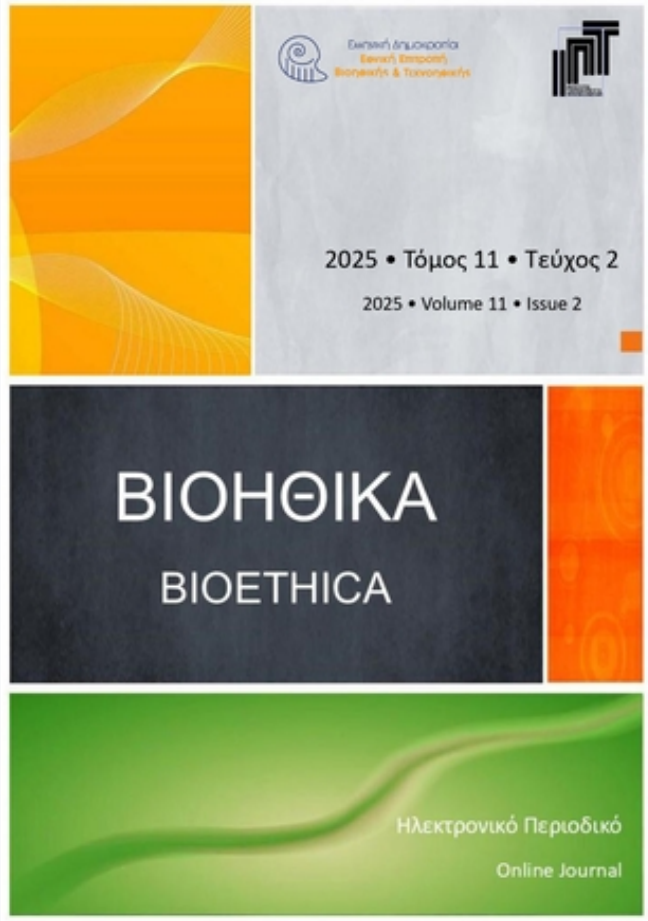
Bioethica

Vol 11, No 2 (2025)

Bioethica



The cybercriminal risks and threats of body-hacking crimes under the legal framework of Budapest Convention

Ahmet Sami Demirezici

doi: 10.12681/bioeth.42841

To cite this article:

Demirezici, A. S. (2025). The cybercriminal risks and threats of body-hacking crimes under the legal framework of Budapest Convention. *Bioethica*, *11*(2), 8–26. https://doi.org/10.12681/bioeth.42841

Πρωτότυπη Εργασία

The cybercriminal risks and threats of body-hacking crimes under the legal framework of Budapest Convention

Ahmet Sami Demirezici[1,2]

[1] Bilkent University, Ankara, Turkey.
[2] Intern, National Commission for Bioethics & Technoethics, Greece.

sami.demirezici@outlook.com

Abstract

In this Article, the Budapest Convention (The Convention on Cybercrime, Council of Europe, ETS No. 185) is put under legal analysis in the scope of risks and threats of cybercrimes against implantable, prosthetic and medical devices, referred to as "Body-Hacking Crimes" according to the terminology of this research. To analyze the Budapest Convention systematically, the risks and threats of "Body-Hacking Crimes" are brought to light under three sub-headings (Body-Hacking, Elements of Cybercrimes, Crimes & Reservations) as the main subjects of this Article. Under the first sub-heading, the term "Body-Hacking" is defined and explained as regards of its usage in the general and criminological literature to describe a new category of cybercrimes, as classified "Body-Hacking Crimes" in this paper. Under the second sub-heading, the elements of cybercrimes are analyzed in regard to the substantive law and human rights provisions of the Budapest Convention and legal loopholes regarding body-hacking crimes are uncovered in these provisions. Though there are multiple elements of cybercrimes required to be analyzed in specific to body-hacking crimes, only three elements (Intention, Non-Authorization, Computer Systems) are evaluated under the second sub-heading due to the inadequate regulations and definitions of these elements in the Budapest Convention. Under the final and third sub-heading, computer-related crimes and reservations regulated in the Budapest Convention are examined in correlation with the hackable nature of implantable, prosthetic and medical devices. Particularly, bodily integrity crimes are brought into the focus for legal analysis of body-hacking crimes inducing bodily damage in the final part of this article. In this study, the substantive-law-oriented and definitional problems of the Budapest Convention are predominantly investigated, which results in pointing out mostly Articles 1-13 of Budapest Convention. Furthermore, the domestic laws and court verdicts, esp. UK, US, France and Dutch cybercrime laws and supreme court decisions, are referred in this study to provide a legal perspective regarding the development of body-hacking crimes in the national legislations.

Keywords: the Budapest Convention; cybercrimes; medical devices; body-hacking; the principle of dual criminality.

Οι κίνδυνοι και οι απειλές του κυβερνοεγκλήματος από εγκλήματα body hacking στο πλαίσιο της Σύμβασης της Βουδαπέστης

Ahmet Sami Demirezici[1,2]

[1] Πανεπιστήμιο Bilkent, Άγκυρα, Τουρκία.
[2] Ασκούμενος, Εθνική Επιτροπή Βιοηθικής και Τεχνοηθικής, Ελλάδα.

Abstract

Στο άρθρο αυτό εξετάζονται από νομική άποψη εγκλήματα στον κυβερνοχώρο κατά εμφυτεύσιμων, προσθετικών και ιατρικών συσκευών, που αναφέρονται ως «εγκλήματα παραβίασης σώματος», σύμφωνα με τη Σύμβαση της Βουδαπέστης (Σύμβαση για το έγκλημα στον κυβερνοχώρο / Συμβούλιο της Ευρώπης). Αναλύονται τα στοιχεία των εγκλημάτων στον κυβερνοχώρο υπό το πρίσμα των διατάξεων του ουσιαστικού δικαίου της Σύμβασης και αποκαλύπτονται τα νομικά κενά που αφορούν τα συγκεκριμένα εγκλήματα στις εν λόγω διατάξεις. Επίσης, εξετάζονται τα εγκλήματα που σχετίζονται με τους υπολογιστές σε συνάρτηση με τις ρυθμίσεις της Σύμβασης για την ευάλωτη φύση των εμφυτεύσιμων, προσθετικών και ιατρικών συσκευών. Ειδικότερα, τα εγκλήματα κατά της σωματικής ακεραιότητας τίθενται στο επίκεντρο της νομικής ανάλυσης. Εξ άλλου, επισημαίνονται εθνικοί νόμοι και δικαστικές αποφάσεις, ιδίως οι νόμοι και οι αποφάσεις των ανώτατων δικαστηρίων του Ηνωμένου Βασιλείου, των ΗΠΑ, της Γαλλίας και των Κάτω Χωρών για τα εγκλήματα στον κυβερνοχώρο, ώστε να μελετηθεί στο συγκεκριμένο πλαίσιο η εξέλιξη των εγκλημάτων σωματικής βίας στα εθνικά νομικά συστήματα.

Λέξεις κλειδιά: Σύμβαση της Βουδαπέστης, εγκλήματα στον κυβερνοχώρο, παραβίαση σώματος, αρχή του διπλού αξιόποινου.

1. Introduction

The integration between body and technology has been improving in correlation with technological developments in biotechnology. The current prostheses, implants, and stimulation devices are more developed and effectively practicable for treating deficient parts of the human body and even enhancing them beyond the edge of human capacity. Moreover, It is no longer a dream to adopt mind-controlled prosthetics, brain-computer interfaces and smart contact lenses, which have succeeded through many examinations and are waiting for industrial production and sale in the near future. Nonetheless, while new technological devices are developed to answer today's problems, they create new risks and threats in parallel with their usage in modern societies. Currently, the most serious threat for medical devices is their hackable nature, and unfortunately, the cybersecurity of these devices is not sufficiently developed to prevent cyberattacks and protect their users 'privacy. Besides technological insufficiencies, legal and administrative remedies are also not well-designed and prepared to deter cybercriminals from illegal access to these devices. Even in the Council of Europe's Convention on Cybercrime (Budapest Convention), which is the most prestigious and accepted Cybercrime Treaty with its 72 party states, there are non-regulated or inadequately regulated parts rendering medical devices and human bodies vulnerable to cyberattacks and leaving cybercriminals released from their actions. In this article, these parts will be spotted and examined in order to assist legislators in eliminating these loopholes and adjusting the Convention more comprehensively. Nonetheless, before the legal examination of the Budapest Convention, the scope of the crimes that are used as the criteria shall be clarified to detect the loopholes in the Budapest Convention. Besides medical devices, prosthetic and implantable devices can also be targeted by cyberattacks which result in serious negative impacts on body functions. Moreover, implantable and prosthetic devices can be used for practical and aesthetic purposes instead of health-related functions, while cyberattacks against them hold the same negative influence on the human body. Since this study aims to deter these consequences by improving the remedial mechanism of the Budapest Convention, the scope of the crimes used as the criteria shall be determined to the extent that covers cybercrimes against all implantable, prosthetic and medical devices, which can create similar consequences to body functions. In the literature, the phrase "hacking human body" is used in the meaning to encompass all cybercrimes against these devices.[1] Hence, the term "body-hacking" is initially analyzed to identify the category of cybercrimes targeting all medical, implantable and prosthetic devices that may have a profound

[1]E. g. Daniel C. Can We Hack the Human Body? LinkedIn, 2022. https://www.linkedin.com/pulse/can-we-hack-human-body-prof-dr-daniel-cebo?utm_source=share&utm_medium=member_ios&utm_campaign=share_via.
Earnhardt R. Hacking the Human Body: The Cyber-Bio Convergance. In Harrigan G. (ed) On the Horizon: Security Challenges at the Nexus of State and Non-State Actors and Emerging/Disruptive Technologies. SMA Periodic Publication, 2019, 32-38. https://nsiteam.com/social/wp-content/uploads/2019/04/DoD_DHS-On-the-Horizon-White-Paper-_FINAL.pdf.
Rauwel G. Body Hackers: Cyber Murders in a Gamer Culture, Kindle: 2015.
Wiles K. Your body is your internet – and now it can't be hacked. Purdue University, 2019. https://www.purdue.edu/newsroom/archive/releases/2019/Q1/your-body-has-internet--and-now-it-cant-be-hacked.html.
Williams S. Three unsafe technologies that could 'hack our bodies'. SecurityBrief UK, 2023. https://securitybrief.co.uk/story/three-unsafe-technologies-that-could-hack-our-bodies.

influence on body functions, as named "Body-Hacking Crimes" in this paper.

2. The Term "Body-Hacking"

2.1. The Primary Meaning of Body-Hacking

Body-hacking refers to the do-it-yourself practice of body modification, made to improve human capacities or change body functions, which intends to expand the boundaries of the human body by surgical implanting of electronic and computing devices into the body.[2] Since the 1990s, it has been promoted and developed due to technological developments and the support of transhumanist and biopunk movements. Especially in parallel to rapid developments in Radio Frequency Identification (RFID) Technology, which uses radio waves to identify people or objects automatically, the body-hacking movement gains more momentum in daily life usage through the adoption of passive RFID implants requiring no battery or any other electric sources implanted in the body.[3] Nonetheless, body-hacking is still an unpopular practice since health facilities do not perform surgeries for body-hacking movement purposes, and self-surgery implantation of devices has low demand for high health risks. As a result, even though there are some technology enthusiasts making self-surgery implantation of devices to modify their bodies for ecstatic or daily usage purposes, the implantation of devices is generally performed for medical purposes to treat bodily disorders or overcome disabilities. On the other hand, RFID implants are vulnerable to cyberattacks like the other types of implantable devices.[4] Hence, although the practice of body-hacking is not addressed in the following parts of the Article, RFID implants adopted for body-hacking purposes are taken up in general and in particular for some cybercrimes against them which are omitted from the jurisdiction of the Budapest Convention.

2.2 Body-Hacking in Criminological Terminology

In general, "hacking" connotes an immoral meaning, being defined as unauthorized and illegal access to systems, networks, or data.[5] Yet,

[2]Giger JC, Gaspar R. A look into future risks: A psychosocial theoretical framework for investigating the intention to practice body hacking. Human Behaviour and Emerging Technologies 2019, 1: 306-307. https://onlinelibrary.wiley.com/doi/epdf/10.1002/hbe2.176.
Jael M. BODY HACKING AND CONCEPTIONS OF CORPOREALITY. Aletheia: The Arts and Science Academic Journal 2022, 2: 52. https://journals.mcmaster.ca/aletheia/issue/view/172/99.

[3]Aubert H. RFID technology for human implant devices. Comptes Rendum Physique 2011, 12: 675-683. https://www.sciencedirect.com/science/article/pii/S1631070511001563.
Mark N Gasson MN, Koops BJ. Attacking Human Implants: A New Generation of Cybercrime. Law, Innovation and Technology 2013, 5: 251-252. http://dx.doi.org/10.5235/17579961.5.2.248.

[4]Kolitz D. Could Someone Hack My Microchip Implant? Gizmodo, 2020, https://gizmodo.com/could-someone-hack-my-microchip-implant-1845216410.

[5]Cambridge Dictionary Online. Hacking. accessed on April 29, 2024.

it can also have an ethical implication in accordance with the context referring to the detection of unintended and deficient parts of a system, network or data and applying them in new and inventive ways to fix these vulnerabilities.[6] In the formation of "body-hacking", hacking primarily adds the latter meaning into this compound word, redefining it in a way that the insufficient and unwanted parts of the body system are adjusted and reconstructed with the process of self-surgery implantation of devices. Nonetheless, it is used in the sense of illegal and unauthorized access to implanted devices and human bodies in the criminological context and literature. In a more ordinary sense, "body-hacking" is also attributed in the criminological literature as the category of cybercrimes targeting implantable, prosthetic and medical devices in parallel to the colloquial meaning of hacking as cyber-offences targeting computer systems.[7] Since the colloquial usage of "body-hacking" reflects the main subject of this study, this term is appealed with a new combined expression as "Body-Hacking Crimes" to stand out its categorical feature and criminal nature.

3. Elements of Cybercrimes

3.1 Intention

Intention is one of the fundamental elements of crimes for the punishment and the conviction of someone in criminal law. As a standard rule, suspects cannot be charged for their actions if they do not intend to engage in criminal behaviors or create unintended effects from their actions. Nevertheless, as an exception to this rule, negligent actions can be criminalized due to the high risk of danger, even if suspects do not intend to act criminally or lead to harmful consequences for someone. In the Budapest Convention, all the crimes mentioned require the intention of criminals in order to be charged against their actions. Nonetheless, body-hacking crimes can result in serious bodily harm up to fatal injuries due to the strong influence of the devices subjected to them on body functions. Especially some medical devices, such as cardiac defibrillators, pacemakers and insulin pumps, can have a decisive role in the stabilization and sustaining of body organ systems, like the blood circulatory system and insulin-glucose system, that a few minutes of their inactiveness can give rise to fatal outcomes. Additionally, undertaking cybercriminal activities against these devices is extremely simple due to their low cybersecurity mechanisms. Until now, only a few cyberattack on medical devices resulting in bodily injury has been detected, yet many studies repeatedly forewarn the users of these devices about how palpable the threat of body-hacking crimes is and

https://dictionary.cambridge.org/dictionary/english/hacking. United Nations Office on Drugs and Crime. Offences against the confidentiality, integrity and availability of computer data and systems. 2019. Accessed on May 1, 2024. https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html.

[6]Erickson J. Hacking: The Art of Exploitation 2nd ed. No Starch Press, 2008: 1. https://repo.zenk-security.com/Magazine E-book/Hacking- The Art of Exploitation (2nd ed. 2008) - Erickson.pdf.

Jael M, *op.cit.*, p. 54.

IBM. What is ethical hacking? Accessed on April 28, 2024. https://www.ibm.com/topics/ethical-hacking.

[7]Claugh J. Principles of Cybercrime 2nd ed. Cambridge University Press, 2015: 31.

how comparatively easy it is to accomplish. At a Blackberry Security Summit in 2015, Blackberry Chief Security Officer David Kleidermacher and security researcher Graham Murphy demonstrated how hackers could shut down infusion pumps and increase or decrease the medication dosage being delivered with just a network cable and a laptop or tablet.[8] According to the research of McAfee security specialist Barnaby Jack, a cyber-attacker does not even need a network cable to disable the alert feature of insulin pumps and dispense a potentially lethal dose of insulin by only using computer software and a custom-built antenna with a range of 300 feet.[9] In a two-year comprehensive study, Scott Erven, the head of information security for Essentia Health, revealed that cyberattackers could also manipulate Bluetooth-enabled defibrillators to deliver random electric shocks to a patient's heart or prevent a medically needed shock from occurring. As regards the implantable cardiovascular defibrillators, Scott Erven especially noted in his article that defibrillators have default and weak passwords to the Bluetooth stacks, like an iPhone pin that can be guessed with ease.[10]

In light of these studies, it is proven that users of implantable, prosthetic and medical devices are at a high health risk, and several measures are required to be taken. The manufacturers of these devices are trying to improve their cybersecurity systems to prevent cyberattacks against them. Nonetheless, enhanced cybersecurity measures can hamper access to these devices in an emergency. Moreover, enhanced cybersecurity systems produce more energy, so they can slow down medical devices and reduce their usable battery life, leading to more surgical operations to replace these devices and their batteries.[11] Hence, manufacturers generally take a cautious approach towards improving the cybersecurity measures of these devices, which results in infrequent upgrading of the cybersecurity mechanisms. As a substitute for the role of the manufacturers, state authorities undertake the burden of measure implantation by executing their legislative and administrative powers. As an example of these measures, some countries criminalize negligent cyberattacks against these devices resulting in bodily harm to increase the caution of hackers intending harmless actions towards the human body, like illegal access to personal data or interference with data not affecting the function of the devices. For instance, in the Section 161septies of the Dutch Criminal Code and the 3ZA Section of the UK Computer Misuse Act 1990, negligent cyber acts causing or creating a risk of death are

[8]Mottle J. Blackberry Offers Insight On Hidden Security Headaches for Patients. Providers, Fierce Heathcare, 2015. https://www.fiercehealthcare.com/mobile/blackberry-offers-insight-hidden-security-headaches-for-patients-providers.

[9]Kostadinov D. Hacking Implantable Medical Devices. INFOSEC INST, 2014: supra note 47. http://resources.infosecinstitute.com/hcking-implantable-medical-devices/ .

[10]Zetter K. It's Insanely Easy to Hack Hospital Equipment. WIRED, 2014. http://www.wired.com/2014/04/hospital-equipment-vulnerable.

[11]Williams PAH, Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Dove Press Medical Devices: Evidence and Research 2015: 311. http://dx.doi.org/10.2147/MDER.S50048.

criminalized with the punishment of imprisonment, monetary sanction, or both. In the 3ZA Section of the UK Computer Misuse Act 1990, negligent cyber attacks causing or creating a significant risk of illness and injury are also penalized with the same punishments. Nonetheless, cybercriminal acts can be carried out outside the jurisdiction of the countries while affecting their residents, which enables foreign cybercriminals to commit crimes without paying off for their actions. Hence, state authorities attempt to provide dual criminality with international conventions to avoid the transnational consequences of cybercrimes. As the most ratified cybercrime convention, the Budapest Convention has a vital role in providing dual criminality between sovereign states. Nonetheless, it doesn't include any provision penalizing negligent acts of cybercrime resulting in bodily harm. Furthermore, it is permitted to restrict the scope of the intention in some cybercrimes by filing reservations to several specific articles in the Budapest Convention. For instance, in Articles 2 and 3, a party country may reserve that the offence shall be committed with dishonest intent or with the intent of obtaining data for illegal access. In regard to negligence and intention, the Convention provides discretionary power to its members to regulate their domestic sanctions in accordance with their legal systems. Nevertheless, this discretionary power creates a significant risk for the users of the devices subjected to body-hacking crimes, contradicting one of the primary purposes of the Convention mentioned in the Preamble as *"to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation"*. Hence, even though this discretionary power can be accepted as a well-placed measure in general, it clearly features an inconsistency with the purpose of the Budapest Convention in particular to body-hacking crimes and requires an adjustment in the Convention in parallel to them.

3.2 Non-authorization and Human Rights

According to Section 1 of the Budapest Convention, every cybercrime necessitates the commission of an act without right. In other words, an act committed with right is not accepted as cybercrime in the Budapest Convention. In the Explanatory Note, though the alternative interpretation by a party state is allowed, the act with right generally refers to *"conduct undertaken with authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is covered by established legal defences, excuses, justifications or relevant principles under domestic laws"*.[12] In domestic laws, both conducts are prescribed and restricted by legislators to avoid legal uncertainty, disproportionality and exploitation of rights. Nonetheless, while legal defences, excuses, justifications or relevant principles are only executed under extraordinary and exceptional circumstances, authority is a general concept exercised frequently in all positions of society. Furthermore, legal defences, justifications, excuses or relevant principles are only applied to natural persons, exceptionally to commercial legal persons, while authority is generally exerted by government institutions, which also encompass legislative bodies regulating their authorities. Hence, the supervision of authority cannot be effectively ensured by domestic laws, which leads societies as a last safeguard to mainly bind their governments with human rights conventions and empower an independent court to detect breaches of these conventions and

[12]Council of Europe. Explanatory Report to the Convention on Cybercrime. European Treaty Series 2001, 185: 8. https://rm.coe.int/16800cce5b.

punish them for their violations. In the Budapest Convention, although no international court has been established or determined for supervision, the Preamble, Article 15[13], and the Explanatory Report of the Budapest Convention refer to international human rights conventions and instruments for providing safeguards and conditions in implementing the Articles. Hence, authorized acts of cybercrimes in Section 1 of the Convention may be legalized only if they do not violate human rights or their limitations regulated in international instruments. In the current international instruments, most human rights are protected due to the tendency of governments to disregard them and the irrevocable harm of their violations against human individuals. Nevertheless, several human rights are not included in these instruments due to the fear of human rights inflation[14] and up-to-date emergence of them in parallel to social, legal, technological changes and developments. Especially in conjunction with the rapid developments in neurotechnology, new category of human rights have arisen recently, known as "neurorights" in the doctrine that serve as a legal shield against crimes affecting neurofunctional stability of individuals. Nonetheless, most of the neurorights have not been involved in international human rights instruments yet. Despite being recognized as the most well-known neurorights, cognitive liberty, the right to psychological continuity and the right to mental privacy are still not mentioned in any human rights instruments.[15] Mental privacy, as also one of the fundamental neurorights, is only mentioned in the Charter of Fundamental Rights of the European Union and the UN Convention on Rights of Persons with Disabilities, which are

[13]According to Article 15, procedural provisions of the Budapest Convention are subjected to conditions and safeguards mentioned in international human rights instruments. Nonetheless, investigative powers of state authorities to preserve, search, seizure, collect and intercept data are regulated in the Convention's procedural law section. Since authorized access or interception of data are also encompassed in investigative power of state authorities, Article 15 is also cited in this sentence.

[14]*"The objectionable tendency to label everything that is morally desirable as 'human right'. The unjustified proliferation of new rights is indeed problematic because it spreads skepticism about all human rights, as if they were merely wishful thinking or purely rhetorical claims. Right inflation is to be avoided because it dilutes the core idea of human rights and distracts from the central goal of human rights instruments, which is to protect a set of truly fundamental human interests, and not everything that would be desirable or advantageous in an ideal world."*
Ienca M, Andorno R. Towards new human rights in the age of neuroscience and neurotechnology. Life Sciences, Society and Policy 2017, 13: 9. https://doi.org/10.1186/s40504-017-0050-1.

[15]Bublitz JC, Merkel R. Crimes Against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination. Criminal Law and Philosophy 2014, 8: 60 51–77. https://doi.org/10.1007/s11572-012-9172-y. Istace T. Protecting the mental realm: What does human rights law bring to the table? Netherlands Quarterly of Human Rights 2023, 41: 216. https://doi.org/10.1177/09240519231211823.
Ligthart S. Towards a Human Right to Psychological Continuity? Reflections on the Rights to Personal Identity, Self-Determination, and Personal Integrity. European Convention on Human Rights Law Review 2024, 5: 205. https://doi.org/10.1163/26663236-bja10092.

found insufficient and criticised for not referring to neurotechnology-related practices or particular harms resulted by malevolently interfering with a person's neuropsychological sphere.[16] Under the current circumstances, even though the well-known fundamental human rights and freedoms, such as the freedom of thought, the right to privacy, etc., lay the foundation for neurorights, they cannot provide sufficient protection for individuals against brain data violations, cyber-attacks to neurosystems, manipulative and authoritative interventions to personal identity, psychology and autonomy. Since the existence of neurorights is built upon the purpose of preventing the similar violations and interventions mentioned in the previous sentence, the inclusion of neurorights in the human rights instruments is required for the ideal protection of individuals against ill-intentioned governments and persons.[17] Nonetheless, as no current human rights instruments contain the neurorights, except mental integrity, in their context, the safeguards and conditions mentioned in the Budapest Convention do not apply to authorized acts of body-hacking crimes which attack or interfere with brain implants and impact the personal autonomy, identity, psychology, brain data and similar aspects of the human mind.

3.3 Computer Systems

In the Budapest Convention, "computer systems" are defined as *"any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data"*. Despite its name, computer systems do not only include computers in their extent. Mobile phones, tablets, Internet of Things (IoT) and medical devices are also within the scope of the term.[18] As a matter of fact, only two functional qualities are required to be recognized as a computer system according to the Convention: being pursuant to a program and performing automatic data processing. Similar to many technological devices, most of the devices subjected to body-hacking crimes hold these qualities and are competent to be acknowledged as computer systems. Nonetheless, some versions of these devices, especially the old ones, are not capable of processing data. For instance, some models of passive RFID implants, cognitive prostheses, DBS devices, pacemakers and cardiac defibrillators can only be qualified as simple data storage devices, not as computer systems.[19] Nevertheless, these devices can still benefit from the legal protection of the Convention since the definition of a computer system includes a group of devices of which at least one device processes data; computers consist of a processing unit and peripherals. Hence, a storage device can be a part of a computer system as a peripheral, which is part of a group of devices.[20] There is a Dutch Supreme Court verdict supporting that a device does not have to possess the mandatory functionalities

[16]Ienco M. Common Human Rights Challenges Raised By Different Applications of Neurotechnologies in the Biomedical Fields. Committee on Bioethics of Council of Europe, 2021: 51-52. https://rm.coe.int/report-final-en/1680a429f3#page51.
[17]Ienca M, Andorno R. *op. cit.*, pp. 23-24.
[18]Claugh J, *op. cit.*, pp. 59-68.
[19]Gasson MN, Koops BJ, *op. cit.*, p. 267.
[20]Council of Europe, *op. cit.*, p. 5.

(storing, processing, and transferring in Dutch Law) of a computer in itself, but rather, the combination of devices constituting a computer system should have these functionalities.[21] In that case, the Convention still provide protection if the implant is considered part of a group of devices. Passive RFID implants can only function in conjunction with a reading device, which has the capacity to process data, resulting in being qualified as part of a computer system. Deep brain stimulation devices, cognitive prostheses, pacemakers, and cardiac defibrillators can also benefit from the protection of the Convention by having the capacity to process data or being part of a group of devices that involves a data-processing device. Nonetheless, the older models of pacemakers and cardiac defibrillators consist only of pulse generators, electrodes, and some small storage capacity devices, making them insufficient to achieve the threshold of a data processing device.[22] Also, interpreting the mentioned devices as part of a computer system is open to the preference of party states. Consequently, no legal assurance exists that all devices exposed to body-hacking crimes will fall within the protective scope of the legal framework established by the Budapest Convention.

4. Crimes & Reservations

4.1 Cybercrimes in the Budapest Convention

In the Budapest Convention, only the common types of cybercrimes are defined and regulated in Article 2 through Article 11. As an international instrument, it is an obligatory characteristic of the Budapest Convention to be flexible and broadly applicable so that state authorities can recognize and enforce them without reluctance. Hence, as the category of cybercrimes that no incident regarding them has been detected yet, it is acceptable that the Council of Europe did not regulate body-hacking crimes and take them into account in the draft process of the Budapest Convention.[23] Nonetheless, body-hacking crimes pose a significant risk to human health and can produce severe bodily damage that may lead to the loss of human life. Even though a few incidents of body-hacking crimes has occurred before, the more prevalent usage of wireless and BCI (Brain-Computer Interface) technology in implantable, prosthetic and medical devices will enhance their hackability potential in the near future. The risks of body-hacking crimes cannot be disregarded due to these reasons; thus, the Budapest Convention still requires several amendments in order to provide full-fledged protection for these device users. As the first proposed amendment, the current cybercrimes pointed out in the Budapest Convention shall be re-regulated to the degree that unquestionably eliminates the risks of body-hacking crimes. In the Convention, several substantive-law provisions involve the risks of body-hacking crimes due to their incompetent regulation. For instance, Article 5, which regulates the cybercrime of system interference, only criminalizes interferences that seriously hinder

[21]Gasson MN, Koops BJ, *op. cit.*, p. 267.
Hoge Raad [Dutch Supreme Court], March 26, 2013, LJN BY9718.
[22]*Idem*, p. 268.

[23]Browning JG, Tuma S, *op. cit.*, p. 638. https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=4183&context=sclr.

the functioning of computer systems. In other words, it permits member states to exempt cyber acts that hinder the functioning of computer systems lightly but induce serious harm or threat to the human body from punishment. As another example, Article 10, which regulates the offences related to infringements of copyright and related rights, penalizes the violations of the rights associated with intellectual property which is expressed in accordance with several international conventions[24] mentioned in this article. Nonetheless, it is questionable whether human thoughts and memories stored in the brain implants must be accepted as expressed per the mentioned conventions. These conventions do not include any clause regarding the automatic expression of human thought or memory stored in brain implants. Hence, it is possible that state authorities interpret these conventions alternatively and decide to exclude the infringement of human thought and memory from the scope of Article 10. Nevertheless, the infringement of human memory and thought can award the perpetrators enormous gains on the economic scale. For instance, a memory of a famous person in his brain implant can be merchandized and distributed like a movie or a documentary, or the thought of an individual stored in his brain implant can lead to a miraculous invention and gain enormous money to its possessor. Even though illegal access to brain implants is penalized under Article 2 of the Budapest Convention, the unlawful economic usage of human memory and thought cannot be criminalized by the following articles of Budapest Convention besides Article 10. Illegal economic use of intellectual property forms another act of crime and might receive more severe punishments due to their important role in the economic and intellectual development of societies. In order to provide just and fair punishment for this cybercriminal act, Article 10 shall be modified to the extent that human thought and memory are protected against intellectual property rights infringements. Hence, an additional intellectual property convention that covers human memory and thought in brain data under the scale of intellectual property rights can be included in the agreements listed in Article 10, or particular regulation in regards to it might be added in this article.

As per the second proposed amendment, body-hacking crimes shall be regulated specifically in the substantive law section of the Budapest Convention. A general provision regarding cybercrimes inducing bodily damage can be inserted for the overall health risks of body-hacking crimes discussed above. Nevertheless, several specific body-hacking crimes possess unique characteristics engendering consequences that extend beyond psychological and physical damage. As an example of these crimes, brainjacking, the exercise of unauthorized control of another's electronic brain implant, shall be explicitly regulated due to its particular consequences on the human body, emotions and autonomy.[25]

[24]Paris Act of 24 July 1971 Revising the Berne Convention for the Protection of Literary and Artistic Works, International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights, WIPO Copyright Treaty and WIPO Performances & Phonograms Treaty.

[25]Pugh J et al. Brainjacking in deep brain stimulation and autonomy. *Ethics and Information Technology*

Similar to other body-hacking crimes, brainjacking can cause physical damage to brain tissue and prevent a programmed medical treatment of brain implants by overcharging them.[26] Nonetheless, it can also lead to the dysfunction of emotional behaviour for the brain implant users and induce unbearable pain in them without requiring a physical injury, such as by increasing the frequency of PAG/PVG stimulation.[27] In the worst scenario, brain implants pave the way for brainjackers to control the users' minds or bodies by sending calibrated electrical impulses to the brain and motor nerves. Brainjackers can influence decisional autonomy in addition to practical autonomy.[28] Though they cannot mainly take part in the decision-making process, they may foster an intention to commit a crime by targeting their users' reward systems and emotions.[29] Nonetheless, brainwashing (mind control) is not recognized as a crime and a legal defence in most national legislations and the Budapest Convention. Except for a few national laws, such as the About-Picard Law in France, most countries do not penalize the sole act of brainwashing and do not uphold it as a legal defence to the criminal liability of the victims.[30] By an explanation of it, it is argued that the theory of brainwashing is not dominantly accepted in the scientific field of psychology due to the lack of empirical data.[31] The traditional methods used in brainwashing and their effects on the victims cannot be empirically analyzed due to the illegality of experimenting with these methods and the complexity of observing the deterministic relationship between them. However, as a procedural obligation, brain implant patients are strictly monitored by advanced medical devices periodically after their surgeries, which provokes the accumulation of great quantities of empirical data. Moreover, the effects of brain implants on the brain are direct, immediate and first-hand. They can also be easily observed due to the trackability of implanted devices and electrodes that monitor

2018, 20: 219. https://doi.org/10.1007/s10676-018-9466-4.

[26]Pycroft L et al. Brainjacking: Implant Security Issues in Invasive Neuromodulation. World Neurosurgery 2016, 92: 455-456. http://dx.doi.org/10.1016/j.wneu.2016.05.010.

[27]*Ibid*, p. 456-457.

Pugh J et al., *op. cit.*, pp. 221-226.

[28]*Ibid*, p. 226.

[29]*Ibidem*.

Pycroft L et al., *op. cit.*, p. 457.

[30]For instance, the criminal legal systems of the United States and Canada, which are the signatory countries of the Budapest Convention, do not acknowledge brainwashing as a legitimate defence for exemption from criminal liability.

Chapman FE. Intangible Captivity: The Potential for a New Canadian Criminal Defense of Brainwashing and Its Implications for the Battered Woman. Berkeley Journal of Gender, Law & Justice 2013, 28: 74. https://doi.org/10.15779/Z38RR1PM1J.

Emory R. Losing Your Head in the Washer – Why the Brainwashing Defense Can Be a Complete Defense in Criminal Cases. Pace Law Review 2010, 30: 1355. https://doi.org/10.58948/2331-3528.1742.

[31]American Psychological Association hasn't accepted brainwashing as a scientific theory.

Warburton ID. The Commandeering of Free Will: Brainwashing as a Legitimate Defense. Capital Defense Journal 2003, 16: 78-79. https://scholarlycommons.law.wlu.edu/wlucdj/vol16/iss1/6.

Emory R, *op. cit.*, p. 1355.

and transmit brain electrical impulses.[32] Hence, the arguments about the unscientific nature of brainwashing methods cannot be given credit in the case of mind control with brain implants. Without any objections, the effects of brain implants on autonomy are scientifically accepted and discussed academically.[33] In a position where science acknowledges the threat of brain implants on autonomy, it would be irrational for legal systems to ignore it and not take any precautions against it. Particularly in conjunction with the rapid advancements in Brain-Computer Interface (BCI) technology, the potential risks associated with brain implants on individual autonomy may increase significantly in the future. Hence, the basic precautionary actions for criminalization and legal excuse for mind manipulation shall at least be taken in domestic laws and the Budapest Convention.

4.2 Bodily Integrity Crimes

As noted in the former section, body-hacking crimes can lead to severe bodily harm due to the impact these devices exert on bodily functions. By deactivation or malfunction of medical devices, a third person can easily interrupt the infusion of a hormone, drug or biochemical fluid that is used to stabilize homeostatic balance or the delivery of electric shocks towards the human heart functioning to correct cardiac arrhythmia, which serves as a reason for that the former US Vice President Dick Cheney disabled his pacemaker's wireless capabilities in 2012.[34] With the aim of mitigating the bodily risks and threats of body-hacking crimes, some state authorities adopt legislative measures to penalize the cybercrimes contributing to bodily harm. For instance, in the 18 U.S. Code §§ 1030(c)(4)(A), the 3ZA Section of the UK Computer Misuse Act 1990 and Section 161sexies of the Dutch Penal Code, cyber acts inducing bodily damage are criminalized with up to imprisonment, monetary penalty, or both. Nonetheless, not all domestic laws encompass specific provisions to penalize these cyber acts. Furthermore, the criteria for bodily damage and acts of cybercrime generally vary in domestic laws. As an example, the 18 U.S. Code §§ 1030 penalizes both illegal access and system interference producing physical injury (at all degree) while the Dutch Penal Code criminalizes only system interferences required to endanger a human life and UK Computer Misuse Act proscribes any unauthorised act in relation to a computer creating a serious injury or illness. As it can be observed from these three different regulations, the application of dual criminality on cybercrimes inducing bodily damage is generally a challenging issue, requiring an international agreement on several points of them to block transnational cybercrimes and secure the users of medical devices to a global extent. Yet, the Budapest Convention and other cybercrime

[32]Jonathan Pugh et al., *op. cit.,* 221.
Quirin T et al. Towards Tracking of Deep Brain Stimulation Electrodes Using an Integrated Magnetometer. Sensors 2021, 21: 1-2. https://doi.org/10.3390/s21082670.

[33]Koivuniemi A, Otto K. When "altering brain function" becomes "mind control". frontiers in SYSTEMS NEUROSCIENCE 2014, 8: 1.
Pugh J et al., *op. cit.*, 219–226.

[34]Browning JG, Tuma S. If Your Heart Skips a Beat, It May Have Been Hacked: Cybersecurity Concerns with Implanted Medical Devices. South Carolina Law Review 2016, 67: 638. https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=4183&context=sclr.

conventions, as being the most effective instrument for ensuring the principle of dual criminality between national legislations, do not include any specific regulation on the subject of cybercrimes inducing bodily harm. In all probability, international commissions can assume that cybercrimes inducing bodily harm are covered by battery or assault laws, which are prescribed and regulated in almost all national legislations, requiring no additional adjustment for cybercrimes inducing bodily harm. Nevertheless, these bodily integrity crimes carry out different features and characteristics than cybercrimes inducing bodily harm. For instance, battery and assault laws subject the crimes that attack the human body, not implants or any other devices. Hence, it is questionable whether implantable, prosthetic and medical devices can be accepted as a part of the body in the context of laws. There are some court cases in France and the Netherlands that treat dental prostheses and teeth implants as an integral part of the human body.[35] By making an analogy, it can be argued that pacemakers, cardiac defibrillators, cochlear implants and other implantable medical devices shall be accepted as part of the human body. Yet, prosthetic limbs are not accepted as human body parts in some court cases, which hardens to protect bionic arms and network cognitive prostheses under the category of assault and battery laws.[36] Moreover, it is also questionable to what extent the neural system is covered by bodily integrity, which determines the legal status of attacks on the brain and neural implants. In the UK and the Netherlands, bodily injuries amount to recognizable psychiatric conditions are covered by battery laws, while the lesser conditions are not.[37] Hence, non-consensual mental infringements, like sending signals to the brain through electronic interference with an implant, are not covered by battery laws, while physical infringements (such as spitting, touching or kissing) are covered by them.[38] Besides setting the bodily borders for the protection of the law, the type of contact and injury for committing battery and assault crimes can also be determinant in the application of cyberattacks against medical implants. Normally, physical contact is sought in the commission of battery and assault crimes, but it is not a prerequisite for the occurrence of them, according to UK and US Case Law.[39] The real

[35]Akmazoglu TB, Chandler JA. Mapping the emerging legal landscape for neuroprostheses: Human interests and legal resources. Hevia M (ed) In Developments in Neuroethics and Bioethics Volume 4. Academic Press, 2021: 83. https://www.sciencedirect.com/science/article/pii/S2589295921000072?ref=cra_js_challenge&fr=RR-1.
Gerechtshof [Court of Appeal] Amsterdam 21 February 2013, LJN BZ2055 [NL].
Rechtbank [District Court] Zutphen 9 February 2010, LJN BL3094.

[36]Browns B. A Farewell to Arms (And Legs): The Legal Treatment of Artificial Limbs. Columbia Journal of Law and Social Problems 2013, 47: pp. 88 and 98. https://jlsp.law.columbia.edu/wp-content/blogs.dir/213/files/2017/03/47-Brown.pdf.
State v. Schaffer, 202 Ariz. 592, 48 P.3d 1202 (Ariz. Ct. App. 2002).

[37]The Crown Prosecutive Service (CPS). Offences against the Person, incorporating the Charging Standard. last updated June 27, 2022. https://www.cps.gov.uk/legal-guidance/offences-against-person-incorporating-charging-standard.
Gasson MN, Koops BJ, *op. cit.*, 273.

[38]*Ibid*, 273.

[39]*Ibid*, 273.

problem is that the criminalization of wounding is much more physically formulated, as it requires an injury that breaks both the outer and inner skin. Attacks on bodily implants will not result in skin injuries, and thus cannot be interpreted as wounding.[40] Nonetheless, several criminal legislations demand crimes to fall within the description of wounding to impose more severe sentences on the criminals. For instance, the Virginia Criminal Code distinguishes wounding (§ 18.2-51) from assault and battery offences (§ 18.2-57), which include only monetary and confinement sanctions for a maximum of 5 years compared to wounding, whose sentence can last up to 20 years imprisonment. Hence, even though national criminal provisions generally encompass general terms to define assault and battery offences,[41] cybercriminals inducing serious bodily damage might not be exposed to severe punishments due to the definitional block of wounding, though they create similar serious consequences to it. In order to provide fair and reasonable punishment to these cybercriminal acts, several national legislations, like Section 20 in UK Offences against the Person Act 1861, broaden the scope of criminal acts in the criminal provisions regarding wounding offences or regulate these acts in separate clauses with similar penalties. Nonetheless, it is not a standard practice between national legislations, so the global nature of cybercrimes can lead to complex applications of their penal codes, which can be concluded with shorter periods of punishment than what the criminals deserve. As mentioned above, the subjects of assault and battery laws are also regulated uniquely based on the laws of countries which produce the same legal complexity and inefficiency in the application of national criminal laws. As a result, mutual cooperation in legislation is also required for assault and battery laws to prevent global consequences of body-hacking crimes.

4.3 Reservations

The incompetent provisions of the Budapest Convention fall body-hacking crimes in a restricted regulatory framework that only apply when they display general characteristics of computer-related crimes prescribed in the Convention. Nevertheless, this narrow scope of the Convention can be limited more by the reservations of the affiliated states allowed in the specific clauses. For instance, according to Article 2, a party state may reserve that the offence of illegal access shall be committed by only infringing security measures. Nonetheless, many implantable medical devices, particularly the older generations, do not possess any security

DPP v K [1990] Cr App R 23.

Fisher v Carrousel Motor Inc., Supreme Court of Texas, 424 S.W.2d 627 (1967).

Bublitz C. The body of law: boundaries, extensions, and the human right to physical integrity in the biotechnical age. Law and the Biosciences 2022, 9: 7. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9621699/pdf/lsac032.pdf.

[40]Gasson MN,Koops BJ, *op. cit.,* 273.

[41]For instance, Dutch Criminal Law uses the term mishandeling (maltreatment) in assault and battery provisions, which allows courts to interpret the actions of criminals broadly.

Teunissen M. Mishandeling versus Assault: A comparative Approach. Master's Thesis, Leiden University, 2017: 38. https://studenttheses.universiteitleiden.nl/access/item:2607954/view.

mechanism at all.[42] Hence, these devices may end up totally defenseless against hacking incidents with this reservation, which may give rise to high-impact disclosures of sensitive personal data stored and processed in these devices. As another example, the criminalization of an attempt to commit any offences mentioned in this Convention can be avoided by the reservation of a party state based on Article 11. By taking account of the possible consequences of an attempted cyberattack against implantable, prosthetic and medical devices with the intention to murder or assault, giving a right to reservation on attempted offences puts the users of these devices at significant risks and under a great fear of injury. As aware of these risks and fear, most countries penalize attempted crimes inducing severe bodily damage in their criminal laws, which seems devaluing the right to reservation regarding attempted body-hacking crimes. Nonetheless, the legal criteria for the acceptance of an action as an attempted crime can vary according to domestic laws. Hence, this situation may lead to a serious struggle for mutual assistance between the party states since the Convention gives party states the right to refuse a request for mutual assistance in its several provisions based on the unfulfillment of dual criminality. For instance, Article 29(4) gives party states a reservation right to refuse data preservation requests based on the unfulfillment of dual criminality for offences other than those established in accordance with Article 2 through Article 11 of the Convention. The condition of dual criminality is deemed to automatically met between the party states for the offences regulated in Article 2 through Article 11, subject to any reservations the affiliated states may have made regarding these offenses where permitted by the Convention.[43] Thereby, the reservation on an attempted crime in Article 11 can invalidate this assumption of dual criminality, retaining the right to refuse data preservation requests. As the preservation request is the key element for other mutual assistance procedures regarding investigative powers, the reservation right on Article 11(3) of the Convention might constitute a significant obstacle for requesting countries in their criminal investigations on attempted cybercrimes. Not only reservation on Article 11(3) but also reservation on Article 4(2) (Data interference only resulting in serious harm), Article 6(3) (Several types of misuse of devices), Article 9(4) (Several offences related to child pornography) and Article 10(3) (Limited circumstances for criminal liability of offenders infringing intellectual property rights) can also constitute this obstacle for requesting countries for their criminal investigations. On account of standard types of cybercrimes, these reservations might be tolerated due to their material kind consequences at most they can result. Nonetheless, body-hacking crimes may lead to health-related consequences that cannot be tolerated in any manner. Hence at least, the Budapest Convention shall keep several reservations out-of-application in regards to body-hacking crimes which endanger human life to the degree that the reservation of them is intolerable in any form.

[42]Núñez CC. Cybersecurity in Implantable Medical Devices. Doctoral Thesis, Universidad Carlos III de Madrid, 2017: 18. chrome://external-file/tesis_carmen_camara_nunez_2018.pdf.

[43]Council of Europe, *op. cit.*, p. 51.

5. Conclusion

In this Research Paper, the cybercriminal risks and threats associated with body-hacking crimes were analyzed under the legal scope of the Budapest Convention. By the conclusion of this legal analysis, it has been figured out that the regulations of the Budapest Convention had been prepared without a comprehensive consideration of cybercrimes against implantable, prosthetic and medical devices in regard to their health-related risks and consequences. By taking the fact that a few incident regarding these cybercrimes has occurred only, it may seem unreasonable to take these crimes into account within the structure of the Budapest Convention. But as explained in this study, these cybercrimes can result in detrimental consequences with respect to human health, personal privacy, bodily integrity and fundamental human rights. Hence, it is crucial to maintain prohibitive and restrictive provisions against these crimes as the precautionary resort within the framework of the Budapest Convention. At this time, it is impossible to alter the textual structure of the Budapest Convention as it has been years since the Budapest Convention was adopted on 23 November 2001. Nonetheless, new protocols regarding the Convention can be issued to modify it, like Council of Europe did in First & Second Protocols to the Budapest Convention. Currently no preparation of Council of Europe is observed for the composition of a new protocol regarding the Budapest Convention. Hence, this study actually serves as a call to action for lawmakers, international organizations, and state officials to proactively integrate these mentioned cybercriminal threats into the legal scope of the Budapest Convention. In that way, it is intended to maintain the Budapest Convention as a relevant and effective tool in the fight against cybercrimes and ensure the proper legal protection of the users of these devices.

Bibliography

Akmazoglu TB, Chandler JA. Mapping the emerging legal landscape for neuroprostheses: Human interests and legal resources. Hevia M (ed) In Developments in Neuroethics and Bioethics Volume 4. Academic Press, 2021: 63-98. https://www.sciencedirect.com/science/article/pii/S2589295921000072?ref=cra_js_challenge&fr=RR-1.

Aubert H. RFID technology for human implant devices. Comptes Rendum Physique 2011, 12: 67-683. https://www.sciencedirect.com/science/article/pii/S1631070511001563.

Browning JG, Tuma S. If Your Heart Skips a Beat, It May Have Been Hacked: Cybersecurity Concerns with Implanted Medical Devices. South Carolina Law Review 2016, 67: 637-677. https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=4183&context=sclr.

Browns B. A Farewell to Arms (And Legs): The Legal Treatment of Artificial Limbs. Columbia Journal of Law and Social Problems 2013, 47: 69-102. https://jlsp.law.columbia.edu/wp-content/blogs.dir/213/files/2017/03/47-Brown.pdf.

Bublitz C. The body of law: boundaries, extensions, and the human right to physical integrity in the biotechnical age. Law and the Biosciences 2022, 9: 1-26. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9621699/pdf/lsac032.pdf.

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

Cambridge Dictionary Online. Hacking. https://dictionary.cambridge.org/dictionary/english/hacking.

Chapman FE. Intangible Captivity: The Potential for a New Canadian Criminal Defense of Brainwashing and Its Implications for the Battered Woman. Berkeley Journal of Gender, Law & Justice 2013, 28: 31-76. https://doi.org/10.15779/Z38RR1PM1J.

Claugh J. Principles of Cybercrime 2nd ed. Cambridge University Press, 2015.

Committee for Scientific and Technological Policy. Recommendation of the Council on

Responsible Innovation in Neurotechnology. OECD, 2019. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457.

Council of Europe. Explanatory Report to the Convention on Cybercrime. European Treaty Series 2001, 185. https://rm.coe.int/16800cce5b.

Daniel C. Can We Hack the Human Body? LinkedIn, 2022. https://www.linkedin.com/pulse/can-we-hack-human-body-prof-dr-daniel-cebo?utm_source=share&utm_medium=member_ios&utm_campaign=share_via.

DPP v K [1990] Cr App R 23.

Earnhardt R. .Hacking the Human Body: The Cyber-Bio Convergance. In Harrigan G. (ed) On the Horizon: Security Challenges at the Nexus of State and Non-State Actors and Emerging/Disruptive Technologies. SMA Periodic Publication, 2019: . https://nsiteam.com/social/wp-content/uploads/2019/04/DoD_DHS-On-the-Horizon-White-Paper-_FINAL.pdf.

Emory R. Losing Your Head in the Washer – Why the Brainwashing Defense Can Be a Complete Defense in Criminal Cases. Pace Law Review 2010, 30: 1337-1359. https://doi.org/10.58948/2331-3528.1742.

Erickson J. Hacking: The Art of Exploitation 2nd ed. No Starch Press, 2008.

https://repo.zenk-security.com/Magazine E-book/Hacking- The Art of Exploitation (2nd ed. 2008) - Erickson.pdf.

Fisher v Carrousel Motor Inc., Supreme Court of Texas, 424 S.W.2d 627 (1967).

Gasson MN, Koops BJ. Attacking Human Implants: A New Generation of Cybercrime. Law, Innovation and Technology 2013, 5: 248-277. http://dx.doi.org/10.5235/17579961.5.2.248.

Gerechtshof [Court of Appeal] Amsterdam 21 February 2013, LJN BZ2055 [NL].

Giger JC, Gaspar R. A look into future risks: A psychosocial theoretical framework for investigating the intention to practice body hacking. Human Behaviour and Emerging Technologies 2019, 1: 306-310. https://onlinelibrary.wiley.com/doi/epdf/10.1002/hbe2.176

Hoge Raad [Dutch Supreme Court], March 26, 2013, LJN BY9718.

IBM. What is ethical hacking? https://www.ibm.com/topics/ethical-hacking.

Ienca M, Andorno R. Towards new human rights in the age of neuroscience and neurotechnology. Life Sciences, Society and Policy 2017, 13: 1-27. https://doi.org/10.1186/s40504-017-0050-1.

Ienco M. Common Human Rights Challenges Raised By Different Applications of Neurotechnologies in the Biomedical Fields. Committee on Bioethics of Council of Europe, 2021. https://rm.coe.int/report-final-en/1680a429f3#page51.

Istace T. Protecting the mental realm: What does human rights law bring to the table? Netherlands Quarterly of Human Rights 2023, 41: 179-260. https://doi.org/10.1177/09240519231211823.

Jael M. BODY HACKING AND CONCEPTIONS OF CORPOREALITY. Aletheia: The Arts and Science Academic Journal 2022, 2: 52-61. https://journals.mcmaster.ca/aletheia/issue/view/172/99.

Kolitz D. Could Someone Hack My Microchip Implant? Gizmodo, 2020, https://gizmodo.com/could-someone-hack-my-microchip-implant-1845216410.

Koivuniemi A, Otto K. When "altering brain function" becomes "mind control". frontiers in SYSTEMS NEUROSCIENCE 2014, 8: 1-6. doi: 10.3389/fnsys.2014.00202

Kostadinov D. Hacking Implantable Medical Devices. INFOSEC INST, 2014. http://resources.infosecinstitute.com/hcking-implantable-medical-devices/.

Ligthart S. Towards a Human Right to Psychological Continuity? Reflections on the Rights to Personal Identity, Self-Determination, and Personal Integrity. European Convention on Human Rights Law Review 2024, 5: 199-229. https://doi.org/10.1163/26663236-bja10092.

Mottle J. Blackberry Offers Insight On Hidden Security Headaches for Patients. Providers, Fierce Heathcare, 2015.

https://www.fiercehealthcare.com/mobile/blackberry-offers-insight-hidden-security-headaches-for-patients-providers.

Núñez CC. Cybersecurity in Implantable Medical Devices. Doctoral Thesis, Universidad Carlos III de Madrid, 2017. chrome://external-file/tesis_carmen_camara_nunez_2018.pdf.

Pugh J et al. Brainjacking in deep brain stimulation and autonomy. Ethics and Information Technology 2018, 20: 219-232. https://doi.org/10.1007/s10676-018-9466-4.

Pycroft L et al. Brainjacking: Implant Security Issues in Invasive Neuromodulation. World Neurosurgery 2016, 92: 454-462. http://dx.doi.org/10.1016/j.wneu.2016.05.010.

Quirin T et al. Towards Tracking of Deep Brain Stimulation Electrodes Using an Integrated Magnetometer. Sensors 2021, 21: 1-18. https://doi.org/10.3390/s21082670.

Rauwel G. Body Hackers: Cyber Murders in a Gamer Culture, Kindle: 2015.

Rechtbank [District Court] Zutphen 9 February 2010, LJN BL3094.

State v. Schaffer, 202 Ariz. 592, 48 P.3d 1202 (Ariz. Ct. App. 2002).

The Crown Prosecutive Service (CPS). Offences against the Person, incorporating the Charging Standard. https://www.cps.gov.uk/legal-guidance/offences-against-person-incorporating-charging-standard.

Teunissen M. Mishandeling versus Assault: A comparative Approach. Master's Thesis, Leiden University, 2017. https://studenttheses.universiteitleiden.nl/access/item:2607954/view.

United Nations Office on Drugs and Crime. Offences against the confidentiality, integrity and availability of computer data and systems. 2019. https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html.

Warburton ID. The Commandeering of Free Will: Brainwashing as a Legitimate Defense. Capital Defense Journal 2003, 16: 73-97. https://scholarlycommons.law.wlu.edu/wlucdj/vol16/iss1/6.

Wiles K. Your body is your internet – and now it can't be hacked. Purdue University, 2019. https://www.purdue.edu/newsroom/archive/releases/2019/Q1/your-body-has-internet--and-now-it-cant-be-hacked.html.

Williams PAH, Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Dove Press Medical Devices: Evidence and Research 2015: 305-316. http://dx.doi.org/10.2147/MDER.S50048.

Williams S. Three unsafe technologies that could 'hack our bodies'. SecurityBrief UK, 2023. https://securitybrief.co.uk/story/three-unsafe-technologies-that-could-hack-our-bodies.

Zetter K. It's Insanely Easy to Hack Hospital Equipment. WIRED, 2014. http://www.wired.com/2014/04/hospital-equipment-vulnerable.