‘I Will Control Your Mind’: The International Regulation of Brain-Hacking

THIBAULT MOULIN*

TABLE OF CONTENTS

 Dr. Thibault Moulin is an Associate Professor at the Catholic University of Lyon (France), and a Research Associate at the Federmann Cyber Security Center of the Hebrew University of Jerusalem (Israel). The views expressed are those of the author. Email: thibault.moulin@mail.huji.ac.il.

ABSTRACT

In the near future, the use of neurotechnologies—like brain-computer interfaces and brain stimulation—could become widespread. It will not only be used to help persons with disabilities or illness, but also by members of the armed forces and in everyday life (e.g., for entertainment and gaming). However, recent studies suggested that it is possible to hack into neural devices to obtain information, inflict pain, induce mood change, or influence movements. This Article anticipates three scenarios which may be challenging in the future—i.e., brain hacking for the purpose of reading thoughts, remotely controlling someone, and inflicting pain or death—and assesses their compliance with international human rights law (i.e., the International Covenant on Civil and Political Rights and the European Convention on Human Rights) and international humanitarian law (Geneva Conventions III and IV, and the First Additional Protocol).

I. INTRODUCTION

The development of neurotechnology—i.e., "devices and procedures used to access, monitor, investigate, assess, manipulate, and/or emulate

the structure and function of the neural systems of natural persons"[1]—may change the daily lives of individuals with disabilities, revolutionize warfare, and be used in the gaming industry. In fact, devices like brain-computer interfaces (BCIs) may help paralyzed people to move or communicate again, allow the remote control of robots and drones ("telepresence"), facilitate communication without the use of vocalized speech ("silent talk"), advance the emergence of modern threat-detection systems, or even guide characters on the screen.[2] Scientists indeed discovered that:

> [E]very action our body performs begins with a thought and with every thought comes an electrical signal, [which] can be received by the Brain-Computer Interface, [consisting of] an electroencephalograph (EEG) or an implanted electrode, which can then be translated, and then sent to the performing hardware to produce the desired action.[3]

In contrast, brain stimulation consists of sending electrical signals into the brain (deep brain stimulation) or the cortical area (transcranial direct current stimulation). The first technique—a "treatment option in patients not responding to less invasive or more conventional therapeutic measures"—shows promising results vis-à-vis Parkinson's disease, dystonia, essential tremor, and chronic pain syndromes.[4] The second technique also shows promising results in the treatment of depression,[5] anxiety,[6] or post-traumatic stress disorder.[7] These techniques may be non-invasive (sensors

1. OECD, RECOMMENDATION OF THE COUNCIL ON RESPONSIBLE INNOVATION IN NEUROTECHNOLOGY 6 (2022).

2. Thibault Moulin, *Doctors Playing Gods? The Legal Challenges in Regulating the Experimental Phase of Human Enhancement*, 54 ISR. L. REV. 236, 258 (2021).

3. Rajesh Uppal, *Military is Developing Brain Control Interfaces Which Allow Controlling UAV Swarms, Fighter Aircrafts and Weaponry with the Speed of Thought*, INT'L DEF. SEC. & TECH. (Mar. 10, 2019), https://idstch.com/technology/biosciences/military-developing-brain-control-interfaces-control-uav-swarms-fighter-aircrafts-weaponry-speed-thought-arrived/ [https://perma.cc/677C-JTMR].

4. Volker Tronnier & Dirk Rasche, *Deep Brain Stimulation*, *in* TEXTBOOK OF NEUROMODULATION: PRINCIPLES, METHODS, AND CLINICAL APPLICATIONS 61, 70 (Helena Knotkova & Dirk Rasche eds., 2015).

5. André Brunoni et al., *Transcranial Direct Current Stimulation for Acute Major Depressive Episodes: Meta-Analysis of Individual Patient Data*, 208 BRIT. J. PSYCH. 522, 522 (2016).

6. Dirson João Stein et al., *Transcranial Direct Current Stimulation in Patients with Anxiety: Current Perspectives,* 16 NEUROPSYCHIATRIC DISEASE TREATMENT 161, 161 (2020).

7. Mohammad Javad Ahmadizadeh et al., *Transcranial direct current stimulation (tDCS) for post-traumatic stress disorder (PTSD): A randomized, double-blinded, controlled trial,* 153 BRAIN RESEARCH BULLETIN 273, 276 (2019).

placed on the head), semi-invasive (electrodes implanted inside the skull), or invasive (implants buried within the brain).[8]

While these neuroscience advances have positive aspects, they also raise significant security and privacy concerns, as devices may be subject to hacking. Potential consequences may vary in severity.[9] For instance, it may just result in the leaking of information. Researchers at the University of Padova suggested:

> [B]rain-computer interfaces are becoming increasingly popular in the gaming and entertainment industries . . . third-party BCI games depend on common APIs [Application Programming Interface] to access BCI devices. Thus, such APIs supply unrestricted access to raw EEG signals for BCI games. Furthermore, such games have complete control over the stimuli that can be presented to users. As a consequence, attackers can display the contents and read their corresponding EEG signals. The content might be videos, pictures, or numbers, which users see when they [are] playing games. Therefore, attackers can specifically design some videos and images shown to users in order to maximize the amount of leaked information.[10]

In fact, the interaction with a BCI consists of a 4-phase cycle.[11] First, there must be an input—that is, "the generation of specific brain activity by the user in response to a stimulus."[12] Second, brain activity must be measured and recorded.[13] Third, "the raw data measured in the second phase should be decoded into its main features and classified."[14] Fourth, decoded signals are translated into an output, and "[o]nce each cycle is completed the user can perceive the feedback resulting from the previous cycle . . . and the next cycle can start."[15] However, it appears that brain-hacking may occur at each phase and generate undesired effects.[16] In a similar fashion, brain stimulators may be hacked to provoke pain, influence emotions, and alter movements.[17]

---

8. PRIYANKA ABHANG ET AL., INTRODUCTION TO EEG- AND SPEECH-BASED EMOTION RECOGNITION 167–69 (2016); Elisabeth Hildt, *Brain-Computer Interaction and Medical Access to the Brain: Individual, Social and Ethical Implications*, 4 STUDIES IN ETHICS, LAW, & TECHNOLOGY 1, 2–3 (2010).

9. *See e.g.*, QianQian Li et al., *Brain-Computer Interface Applications: Security and Privacy Challenges* 4 (2015).

10. QianQian Li et al., *Brain-Computer Interface Applications: Security and Privacy Challenges,* 4 (2015).

11. Marcello Ienca & Pim Haselager, *Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity*, 18 ETHICS INF. TECHNOL. 117, 121 (2016).

12. *Id*.

13. *Id*.

14. *Id*.

15. *Id*.

16. *Id.*

17. Laurie Pycroft et al., *Brainjacking - Implant Security Issues in Invasive Neuromodulation*, 92 WORLD NEUROSURGERY 454, 456–57 (2016).

The purpose of this Article, then, consists of anticipating three future scenarios of "brain-hacking," and in determining how existing rules may adapt to regulate them. In particular, attention will be given to the application of international human rights law (IHRL), with specific focus on the International Covenant on Civil and Political Rights (ICCPR)[18] and the European Convention of Human Rights (ECHR).[19] Additionally, international humanitarian law (IHL) will be analyzed with considerations centered around the Geneva Conventions III and IV,[20] as well as the First Additional Protocol.[21] These scenarios include reading thoughts, remotely controlling an individual, and inflicting pain or death.[22]

It is worth mentioning what this Article is not supposed to do: it does not focus on the rights of enhanced soldiers and the return of veterans to

18. International Covenant on Civil and Political Rights ("ICCPR"), Dec. 10, 1966, 999 UNTS 171.

19. European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR"), Nov. 4, 1950, 213 UNTS 221.

20. Geneva Convention Relative to the Treatment of Prisoners of War ("Geneva Convention III"), Aug. 12, 1949, 75 UNTS 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War ("Geneva Convention IV"), Aug. 6, 1949, 75 UNTS 287.

21. Additional Protocol to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts ("Additional Protocol I"), June 8, 1977, 1125 UNTS 3.

22. Potential scenarios were flagged by some authors in the past: Ellen McGee, *Should There Be a Law - Brain Chips: Ethical and Policy Issues*, 24 T. M. COOLEY L. REV. 81, 88–89 (2007); Ellen M. McGee & Gerald Maguire, *Ethical Assessment of Implantable Brain Chips,* BIOETHICS & MEDICAL ETHICS (2001), https://www.bu.edu/wcp/Papers/Bioe/BioeMcGe.htm [https://perma.cc/V4UF-3FBV]; Armin Krishnan, *From Psyops to Neurowar: What Are the Dangers?*, ISAC-ISSS 1, 9 (2014), https://cupdf.com/document/from-psyops-to-neurowar-what-are-the-dangers-2019-12-29-2-from-psyops-to-neurowar.html [https://perma.cc/CB4W-UZQK].

civilian life,[23] weapons review,[24] responsibility and self-incrimination,[25] biomedical research,[26] or EU law.[27] It is also notable that this study relies on a basic premise—i.e., that persons resorting to brain stimulation or equipped with BCIs remain human beings and as such, enjoy the rights protected by IHRL and IHL.[28]

Against this background, this Article is structured as follows. In the next section, IHRL, as it applies to brain-hacking, is further explained. In particular, doubt is cast on the notion that extraterritorial jurisdiction is exercised in situations where a State reads someone's thoughts, remotely

---

23. Heather Harrison Dinniss & Jann Kleffner, *Soldier 2.0: Military Human Enhancement and International Law*, 92 INT'L L. STUD. SER. U.S. NAVAL WAR COL. 432 (2016); Matthew Beard, Jai Galliott & Sandra Lynch, *Soldier Enhancement: Ethical Risks and Opportunities*, AUSTL. ARMY J., Autumn 2016, at 5, 15–16; Patrick Lin, Max Mehlman & Keith Abney, *Enhanced Warfighters: Risk, Ethics, and Policy* 1, 85 (2013), http://ethics.calpoly.edu/ Greenwall_report.pdf [https://perma.cc/8NBR-EP5M]; Amanda McAllister, *Cybernetic Enhancement of Soldiers: Conserving Hors de Combat Protections for Combatants under the Third Geneva Convention*, 7 J. L. & CYBER WARFARE 67, 90–91 (2019); Yahli Shereshevsky, *Are All Soldiers Created Equal? On the Equal Application of the Law to Enhanced Soldiers,* 61 VA. J. INT'L L. 271(2021).

24. Luke Chircop & Rain Liivoja, *Are Enhanced Warfighters Weapons, Means, or Methods of Warfare*, 94 INT'L L. STUD. SER. U.S. NAVAL WAR COL. 161 (2018); *see also* Justin McClelland, *The review of weapons in accordance with Article 36 of Additional Protocol I*, 85 INT'L REV. RED CROSS 397 (2003); VINCENT BOULANIN & MAAIKE VERBRUGGEN, ARTICLE 36 REVIEWS—DEALING WITH THE CHALLENGES POSED BY EMERGING TECHNOLOGIES (2017), https://www.sipri.org/sites/default/files/2017-12/sipri_bp_1712_ article_36_compendium_2017.pdf [https://perma.cc/PT4S-VZJQ]; William Boothby, *How Will Weapons Reviews Address the Challenges Posed by New Technologies*, 52 MIL. L. & L. WAR REV. 37 (2013); Natalia Jevglevskaja, *Weapons Review Obligation under Customary International Law*, 94 INT'L L. STUD. SER. U.S. NAVAL WAR COL. 186 (2018); Thibault Moulin, *No More Humans? Cybernetically-Enhanced Soldiers Under the Legal Review of Article 36*, 8 J. L. & CYBER WARFARE 59 (2021).

25. Gregor Noll, *Weaponising neurotechnology: international humanitarian law and the loss of language*, 2 LONDON REV. INT'L L. 201, 212–14 (2014); Stephen E. White, *Brave New World: Neurowarfare and the Limits of International Humanitarian Law*, 41 CORNELL INT'L L.J. 177 (2008); Roberto Andorno & Marcello Ienca, *Towards new human rights in the age of neuroscience and neurotechnology*, 13 LIFE SCI., SOC'Y & POL'Y, no. 5, at 1, 16–17 (2017).

26. Moulin, *supra* note 2.

27. Eleni Kosta & Diana Bowman, *Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants*, *in* HUMAN ICT IMPLANTS: TECHNICAL, LEGAL & ETHICAL CONSIDERATIONS 97 (Mark Gasson, Eleni Kosta & Diana Bowman eds., 2012); Andreas Kuersten & Roy Hamilton, *The Brain Cognitive Enhancement Devices and European Regulation*, 1 J.L. & BIOSCI. 340 (2014).

28. For discussions on this issue, see David Lawrence, *To What Extent Is the Use of Human Enhancements Defended in International Human Rights Legislation*, 13 MED. L. INT'L 254, 263–65 (2013) https://journals.sagepub.com/doi/ pdf/10.1177/0968533214520845; *see also* Guy Eden, *Targeting Mr. Roboto: Distinguishing Humanity in Brain-Computer Interfaces*, 228 MIL. L. Rev. (2020), https://tjaglcs.army.mil/en/mlr/targeting-mr.-roboto-distinguishing-humanity-in- brain-computer-interfaces [https://perma.cc/PUQ4-YBD8].

controls an individual, inflicts pain or death. Where the ICCPR and the ECHR apply it appears that brain-hacking would be contrary to some rights protected by the conventions, like the right to life, the prohibition of torture, cruel, inhuman or degrading treatment, and freedom of thought. Some positive obligations would also arise in that context; they are explored in Section 2. In the third section, discussion turns to the application of IHL. Section 3 further explains that Geneva Conventions III and IV, as well as the First Additional Protocol, though may have little to say about the access to someone's thoughts, regulate some situations where a civilian or someone hors-de-combat is remotely controlled, inflicted pain, or killed. Finally, Section 4 concludes the Article.

II. THE POTENTIAL CONTRADICTION OF BRAIN-HACKING WITH INTERNATIONAL HUMAN RIGHTS LAW

The application scope of the ICCPR and the ECHR are expressly mentioned in the conventions. According to Article 2(1) ICCPR "[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant."[29] Article 1 ECHR underlines that "[t]he High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in . . . this Convention."[30] If there is little doubt that States Parties shall secure these rights within their own territories, the question of extraterritorial application is challenging. In fact, a State could access the neural devices of persons beyond its own borders. The question which arises, then, is the following: is transborder brain-hacking tantamount to the exercise of jurisdiction? As discussed below in Section IIA, the hacking is not. Then, where they are applicable, both the ICCPR and the ECHR give rise to "negative" obligations—i.e., to refrain from interfering with these rights—and "positive" obligations—i.e., to adopt measures to safeguard them.[31] Section IIB demonstrates that by virtue of their negative obligations, States shall indeed refrain from committing brain-hacking, which is contrary to the conventions. Last but not least, the neural devices of individuals within the territory or jurisdiction

29. ICCPR, *supra* note 18, art. 2(2).
30. ECHR, *supra* note 19, art. 1.
31. *See* JEAN-FRANÇOIS AKANDJI-KOMBÉ, HUMAN RIGHTS HANDBOOK, NO. 7, POSITIVE OBLIGATIONS UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS (2007), https://rm.coe.int/168007ff4d [https://perma.cc/YW99-YKEU].

of a State Party could be hacked by national and foreign actors. In this context, arguments that States have positive obligations are put forth in Section II.C, as well as recommendations for the adoption of some measures to comply with those obligations.

A. The Absence of Extraterritorial Jurisdiction in the Event of Mere Brain-Hacking

The extraterritorial application of human rights conventions is controversial. It is accepted that the conventions may apply abroad, but the conditions to be met are disputed. Through the exploration of case law of the Human Rights Committee (HRC) and the European Court of Human Rights (ECtHR), the fact that extraterritorial jurisdiction does not exist where mere brain-hacking occurs becomes apparent. This is the case for the three situations mentioned above: (1) reading thoughts, (2) controlling an individual, and (3) inflicting pain or death.

1. Reading Thoughts

The HRC progressively acknowledged that subject to some conditions, the ICCPR does apply extraterritorially. The so-called "spatial" model of extraterritorial jurisdiction—where a State has *de facto* control over a territory—is the least problematical situation. Under these circumstances, the protection by the ICCPR extends to individuals within territories controlled by a State Party.[32] The so-called "personal" model of extraterritorial jurisdiction—where a State would not have control over a territory but over individuals—is more problematic.[33] In *Lopez-Burgos*, the Committee found that "it would be unconscionable to so interpret the responsibility under Article 2 of the Covenant as to permit a State Party toperpetrate violations of the Covenant on the territory of another State, which violations

32. *See* Concluding Observations of the Human Rights Committee: Israel, U.N. Hum. Rts. Comm. on Its Sixty-Third Session, U.N. Doc. CCPR/C/79/Add.93, at ¶ 10 (1998), https://www.refworld.org/docid/3ae6b0284.html [https://perma.cc/J78E-RSLB]; see also Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶¶ 109–12 (July 9).

33. There are some alternative views though. According to Dario Rossi D'Ambrosio, the concept of State jurisdiction must be understood as a relationship of power between the State and the individual, regardless of situations of control over territory or individuals, Dario Rossi D'Ambrosio, *The Human Rights of the Other: Law, Philosophy and Complications in the Extra-Territorial Application of the ECHR*, 2 SOAS L.J. 1 (2015); According to Hugh King, "'jurisdiction' in the ICCPR and ECHR should be understood as arising when a state has lawful competence to act extraterritorially under rules of international law, as well as when a state acts beyond that competence to a person's detriment." Hugh King, *Extraterritorial Human Rights Obligations of States*, 9 HUM. RTS. L. REV. 521, 556 (2009).

it could not perpetrate on its own territory."[34] This approach was confirmed in *Celiberti de Casariego*.[35] In *Lichtensztejn v. Uruguay,* the HRC decided that the issue of a passport to a Uruguayan citizen who lived in Mexico was "clearly a matter within the jurisdiction of the Uruguayan authorities."[36] In 2004, the HRC had the opportunity to clarify this decision in *General Comment No. 31* which states: "[a] State Party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party."[37] Remote access to data and the issue of jurisdiction became topical with the emergence of bulk surveillance and the espionage scandal involving the NSA. In 2014, the HRC adopted a less restrictive view and found that the United States had to "[t]ake all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant."[38] Later that year, the Office of the United Nations High Commissioner for Human Rights (OHCHR) attempted to reconcile these approaches, and declared:

> The notions of "power" and "effective control" are indicators of whether a State is exercising "jurisdiction." . . . It follows that digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications

34. U.N. Hum. Rts. Comm., Lopez-Burgos v. Uruguay, Commc'n No. R.12/52, U.N. Doc. Supp. No. 40 (A/36/40), ¶ 12.3 (1981), http://hrlibrary.umn.edu/undocs/session36/12-52.htm [https://perma.cc/LK5B-TYZ4].

35. U.N. Hum. Rts. Comm., Celiberti de Casariego v. Uruguay, Commc'n No. 56/1979, U.N. Doc. CCPR/C/OP/1, ¶ 10.3 (1984), http://hrlibrary.umn.edu/undocs/html/56_1979.htm [https://perma.cc/ZL65-9P9G].

36. U.N. Hum. Rts. Comm., Lichtensztejn v. Uruguay, Commc'n No. 77/1980; U.N. Doc. CCPR/C/18/D/77/1980 (1983), http://www.worldcourts.com/hrc/eng/decisions/1983.03.31_Lichtensztejn_v_Uruguay.htm [https://perma.cc/VCZ2-ZFHY].

37. The HRC also mentioned that "[t]his principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained, such as forces constituting a national contingent of a State Party assigned to an international peacekeeping or peace-enforcement operation." *See also* Thibault Moulin, *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, OXFORD INT'L ORG., Apr. 7, 2017, OXIO 198, https://lawschool.westlaw.com/Files/Download/18693058/131171.pdf?serve=true [https://perma.cc/NQ38-VUEK].

38. U.N. Hum. Rts. Comm., *Concluding Observations on the Fourth Periodic Report of the United States of America*, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014), https://www.refworld.org/docid/5374afcd4.html [https://perma.cc/23RM-RA74].

> infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure.[39]

The jurisprudence of the HRC—in particular *Lopez-Burgos, Celiberti de Casariego* and the *2014 Concluding Observations on the United States*—led some experts to suggest that State Parties have negative obligations abroad.[40] If this proved to be true, then State Parties shall refrain from interfering with the rights protected by the ICCPR in any circumstances—including when they read someone's thoughts. However, the case law of the HRC is evolving and this concept remains controversial.[41] The only certainty is that extraterritorial jurisdiction exists where someone is "within the power or effective control" of a State Party—which is arguably not the case where the individual's thoughts are (remotely) read. In fact, the OHCHR said that "power or effective control in relation to digital communications infrastructure" is exercised where "direct tapping or penetration of that infrastructure" occurs (i.e., where physical access is secured). By analogy, this means that States Parties shall not interfere with the ICCPR where they have physical access to a person's neural device.

Regarding the ECHR, the European Court and the European Commission of Human Rights also acknowledged the existence of a spatial and personal model of extraterritorial jurisdiction. In *Loizidou*, the Court declared that the responsibility of a State Party may arise where, as a consequence of a lawful or unlawful military action, "it exercises effective control of an area outside its national territory."[42] This obligation to secure

---

39. Hum. Rts. Comm., Rep. of the Off. Of the U.N. High Comm'r for Hum. Rts. on Its Twenty-Seventh Session, U.N. Doc. A/HRC/27/37, ¶¶ 33–34 (2014), https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf [https://perma.cc/CM8J-TGU9] [hereinafter Rep. of the OHCHR].

40. MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLE & POLICY 210–16 (2011) [https://perma.cc/M689-9WB2]; RUSSEL BUCHAN, CYBER ESPIONAGE AND INTERNATIONAL LAW 100 (2018); Jessica Lynn Corsi, *Drone Deaths Violate Human Rights: The Applicability of the ICCPR to Civilian Deaths Caused by Drones*, 6 INT'L HUM. RTS. L. REV. 205, 225 (2017), https://heinonline-org.sandiego.idm.oclc.org/HOL/PDFsearchable?handle=hein.journals/inthurlr6&collection=journals&section=14&id=&print=section&sectioncount=1&ext=.pdf&nocover=&display=0 [https://perma.cc/QR8H-HDT9].

41. Ibrahim Kanalan, *Extraterritorial State Obligations beyond the Concept of Jurisdiction*, 19 GERMAN L.J. 43, 52 (2018), https://www.cambridge.org/core/services/aop-cambridge-core/content/view/AD1195AA5924DED29924E01CBFF487CD/S2071832200022598a.pdf/extraterritorial-state-obligations-beyond-the-concept-of-jurisdiction.pdf [https://perma.cc/B3DG-NAAJ]; Yuval Shany, *Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law*, 7 L. & ETHICS HUM. RTS. 47 (2013), https://heinonline-org.sandiego.idm.oclc.org/HOL/PDFsearchable?handle=hein.journals/lehr7&collection=journals&section=6&id=&print=section&sectioncount=1&ext=.pdf&nocover=&display=0 [https://perma.cc/G6FR-YE3P].

42. Loizidou v. Turkey, 20 Eur. Ct. H.R. 99, ¶ 62 (1995), https://www.refworld.org/cgi-bin/texis/vtx/rwmain?page=printdoc&docid=402a07c94 [https://perma.cc/MGL5-YMTF].

the application of the ECHR "derives from the fact of such control whether it be exercised directly, through its armed forces, or through a subordinate local administration."[43]

In *Cyprus v. Turkey*, the Commission stated that "the High Contracting Parties are bound to secure the said rights and freedoms to all persons under their actual authority and responsibility, whether that authority is exercised within their own territory or abroad."[44] Again, the level of control on individuals seems quite intensive.[45]

In *Bankovic*, where NATO's aerial bombardment of Yugoslavia resulted in the death of civilians,[46] the Court rejected the applicants' submission, which was allegedly "tantamount to arguing that anyone adversely affected by an act imputable to a Contracting State, wherever in the world that act may have been committed or its consequences felt, is thereby brought within the jurisdiction of that State for the purpose of Article 1 of the Convention."[47]

In *Al-Skeini*, the Court agreed that "in certain circumstances, the use of force by a State's agents operating outside its territory may bring the individual thereby brought under the control of the State's authorities into the State's Article 1 jurisdiction."[48] However, it "does not consider that jurisdiction . . . ar[ises] solely from the control exercised by the Contracting State over the buildings, aircraft or ship in which the individuals [are] held. What is decisive in such cases is the exercise of physical power and control over the person in question."[49] Therefore, it does not seem that extraterritorial jurisdiction is exercised where an individual's thoughts are merely read.

2. Controlling Someone

Establishing jurisdiction becomes problematic where access to someone's neural device is not only used to read their thoughts, but to take control of

43. *Id*.
44. Cyprus v. Turkey, App. No. 788/60, 4 Eur. Comm'n H.R. Dec. & Rep. 136 (1975), https://hudoc.echr.coe.int/eng?i=001-74811 [https://perma.cc/C2NK-HJJY].
45. Shany, *supra* note 41, at 60.
46. Bankovic v. Belgium, 2001-XII Eur. Ct. H.R. 333, 335, https://hudoc.echr.coe.int/eng?i=001-22099 [https://perma.cc/W8EV-D47R].
47. *Id*. at 356.
48. Al-Skeini v. UK, App. No. 55721/07, Eur. Ct. H.R. ¶ 136 (2011), https://www.refworld.org/pdfid/4e2545502.pdf [https://perma.cc/R4TJ-FLJK].
49. *Id*.

their body. Arguably, this would mean the remotely-controlled person would be at the mercy of the hacker as the degree of control over this person would be similar to when an individual is drugged or coerced into doing something at gunpoint. However, starting with the ECHR and the ECtHR, it seems that personal extraterritorial jurisdiction has only been acknowledged in situations where state agents were abroad and exercised physical pressure on an individual. In *Al-Skeini*,[50] the ECtHR found it "clear that, whenever the State, through its agents, exercises control and authority over an individual, and thus jurisdiction, the State is under an obligation under Article 1 to secure to that individual the rights and freedoms . . . of the Convention that are relevant to the situation of that individual."[51] Yet, the situations of extraterritorial control contemplated by the Court in *Al-Skeini* are very different from the situation where someone is (remotely) controlled. First, the Court found that the acts of diplomatic and consular agents, "who are present on foreign territory, may amount to an exercise of jurisdiction when these agents exert authority and control over others."[52] Second, extraterritorial jurisdiction exists when a Contracting State "exercises all or some of the public powers normally to be exercised" on a foreign territory, "through the consent, invitation or acquiescence of the Government of that territory."[53] Third, the Court considered that control "over the buildings, aircraft or ship in which the individuals were held" was not enough—as "[w]hat is decisive in such cases is the exercise of physical power and control over the person in question."[54] Power and control, then, must be "physical." Following the Court's ruling, the remote control of someone would then not be tantamount to extraterritorial

50. For doctrinal discussions of the approach to jurisdiction in this case, see generally: Marek Szydlo, *Extra-Territorial Application of the European Convention on Human Rights after Al-Skeini and Al-Jedda*, 12 INT'L CRIM. L. REV. 271, 283–91 (2012), https://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=75005224&S=R&D=aph&EbscoContent=dGJyMNHX8kSeqLU4v%2BvlOLCmsEqep7ZSrq64TLOWxWXS&ContentCustomer=dGJyMPPk547x2rmF39%2FsU%2BPa8QAA [https://perma.cc/FF4Q-T5B7]; Samantha Besson, *The Extraterritoriality of the European Convention on Human Rights - Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to*, 25 LEIDEN J. INT'L L. 857 (2012), https://plus-lexis-com.sandiego.idm.oclc.org/api/permalink/00efc35a-6a5f-4100-8876-83037754ca51/?context=1530671 [https://perma.cc/7QHL-4CE4]; Alex Conte, *Human Rights beyond Borders: A New Era in Human Rights Accountability for Transnational Counter-Terrorism Operations*, 18 J. CONFLICT & SEC. L. 233, 233–57 (2013), https://web-p-ebscohost-com.sandiego.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=0&sid=53401107-bdaa-4ad9-a203-b7eed55d2b4f%40redis [https://perma.cc/ED8H-DEHB].

51. Al-Skeini v. UK, App. No. 55721/07, Eur. Ct. H.R. ¶ 137 (2011), https://www.refworld.org/pdfid/4e2545502.pdf [https://perma.cc/R4TJ-FLJK].

52. *Id.* ¶ 134.

53. *Id.* ¶ 135.

54. *Id.* ¶ 136.

jurisdiction. Further, the HRC's and OHCHR's position in "power" and "effective control" suggests the results would not be different under the ICCPR, given physical access to the brain is required.

3. Inflicting Pain or Death

Outside the context of occupation, the HRC has never affirmed that shooting or remotely inflicting pain to an individual sufficiently constituted exercise of personal control over someone.[55] For instance, the Committee did not tackle the issue of jurisdiction in the *2014 Concluding Observations on the United States*, even though concerns had been raised regarding the use of drones.[56] In contrast, the ECtHR had the opportunity to do so in the *Bankovic* and *Andreou* cases. As mentioned above, the situation in *Bankovic* arose when a building was hit by a missile launched by an aircraft of the NATO forces, which resulted in the death of several civilians.[57] The Court declined jurisdiction, and eventually stated in *Al-Skeini* that "[w]hat is decisive in such cases is the exercise of physical power and control over the person in question."[58] In *Andreou*, a woman was shot by Turkish agents at the border between Southern and Northern Cyprus.[59] The Court acknowledged that "in exceptional circumstances, the acts of Contracting States which produce effects outside their territory and over which they exercise no control or authority" may be tantamount to extraterritorial jurisdiction.[60] However, this conclusion resulted from a careful examination of the situation. The ECtHR noted that the Turkish agents were within the territory of the Turkish Republic of Northern Cyprus when they shot Ms. Andreou, who "was standing outside the neutral UN buffer zone and in

55. For a different opinion see NILS MELZER, TARGETED KILLING IN INTERNATIONAL LAW 137–39 (2008), https://academic-oup-com.sandiego.idm.oclc.org/book/3153. For situations where state agents exercised authority and control on persons abroad see: Issa and others v. Turkey, App. No. 31821/96, Eur. Ct. H.R. (2005); Pad and others v. Turkey, App. No. 60167/00, Eur. Ct. H.R. (2007).

56. *See* U.N. H.R.C., *Concluding Observations on the Fourth Periodic Report of the United States of America*, ¶ 9, CCPR/C/USA/CO/4, (2014), https://www.refworld.org/docid/5374afcd4.html [https://perma.cc/KLB4-9TAX].

57. Bankovic v. Belgium, 2001-XII Eur. Ct. H.R. 333, 335, https://hudoc.echr.coe.int/eng?i=001-22099 [https://perma.cc/W8EV-D47R].

58. Al-Skeini v. UK, App. No. 55721/07, Eur. Ct. H.R. ¶ 136 (2011), https://www.refworld.org/pdfid/4e2545502.pdf.

59. Andreou v. Turkey, App. No. 45653/99, Eur. Ct. H.R. at 10–11, (June 3, 2008), http://hudoc.echr.coe.int/app/conversion/docx/?library=ECHR&id=001-88068.

60. *Id*.

close vicinity to the Greek-Cypriot National Guard checkpoint."[61] The Court found that "[u]nlike the applicants in the Bankovic and Others case," she was within "territory covered" by the Convention.[62] It concluded:

> Even though the applicant had sustained her injuries in territory over which Turkey exercised no control, the opening of fire on the crowd from close range, which was the direct and immediate cause of those injuries, had been such that the applicant should be regarded as "within [the] jurisdiction" of Turkey within the meaning of Article 1 of the Convention.[63]

However, the Court never acknowledged that shooting a person was sufficient to establish extraterritorial jurisdiction. This means that where pain or death is remotely inflicted on someone, this person would probably not be within "territory covered" by the Convention.

B. The Contradiction Between Brain-Hacking and the Negative Obligations of States Parties

The rights defined by the ICCPR and the ECHR must be secured both within the territory of States Parties and abroad, where they have (spatial or personal) extraterritorial jurisdiction. As mentioned above, it is doubtful that extraterritorial jurisdiction exists where someone's neural device is targeted by a State Party. If the contrary proves to be true, however, these rights must be secured too. Below, the compliance of brain-hacking with relevant provisions from the ICCPR and the ECHR is assessed, and it is demonstrated that (1) reading thoughts, (2) controlling someone, and (3) inflicting pain or death—are often unlawful.

1. Reading Thoughts

Where someone's thoughts are read, the right to privacy (Articles 8 ECHR and 17 ICCPR) and freedom of thought (Articles 9 ECHR and 19(1) ICCPR) may be relevant. An analysis of these provisions reveals a paradoxical outcome: (a) accessing someone's thoughts is not always contrary to the right to privacy—under which derogations are permissible —but (b) it would be *ipso facto* contrary to the freedom of thought— a freedom which cannot be derogated from.

---

61. *Extra-territorial Jurisdiction of State Parties to the European Convention on Human Rights*, EUR. CT. OF HUM. RTS., (July 2018), https://www.echr.coe.int/documents/fs_extra-territorial_jurisdiction_eng.pdf [https://perma.cc/4UGW-V353].

62. *Id*.

63. *Id*.

a. The Right to Privacy

In contrast with the freedom of thought, which is absolute, the right to privacy may be derogated from. The ECtHR and the HRC defined a three-step test to determine if the breach of a protected right occurred. First, the existence of an interference must be assessed.[64] Second, there must be analysis as to whether the interference was in accordance with the law (ECtHR),[65] or if it was arbitrary and/or unlawful (HRC).[66] Third, it must determine if the interference was necessary in a democratic society, in relation to the legitimate aim sought (ECtHR),[67] or of it was proportionate to a legitimate aim (HRC).[68] Below, this Article applies this three-step test to the situation where one's thoughts are read.

Each type of surveillance does not necessarily amount to an interference. For instance, the ECtHR found that there is no interference where individuals are monitored in a public place (if there is no recording).[69] However, the "recording of data" and the "systematic or permanent nature of the record" may result in an interference.[70] Interferences also exists where employees are subject to covert and non-covert surveillance on the workplace,[71] and where police enter and search an individual's home. However, it may be argued that the physical location of where someone's thoughts are read—at work, at home, or in a public location—is of little interest to determine the existence of an interference. It is more interesting to remember that, in the opinion of the Court, an interference occurs where someone's personal information relating to telephone, e-mail and Internet usage

64. UN International Covenant on Civil and Political Rights, Human Rights Committee, Views Adopted by the Committee under Article 5(4) of the Optional Protocol, concerning communication No. 2387/2014, UN Doc. CCPR/C/117/D/2387/2014, ¶ 8.7 (2017), https://juris.ohchr.org/en/Search/Details/2197 [https://perma.cc/JG2A-2X9L].

65. Silver and others v. UK, 5 EHRR 347, ¶¶ 85–88 (ECtHR, 1983).

66. Views Adopted by the Committee under Article 5(4) of the Optional Protocol, concerning communication No. 2387/2014, *supra* note 64, ¶ 8.7.

67. S and Marper v. UK, 48 EHRR 50, ¶ 118 (ECtHR, 2009).

68. Views Adopted by the Committee under Article 5(4) of the Optional Protocol, concerning communication No. 2387/2014, *supra* note 64, ¶ 8.11.

69. Peck v. UK, 36 EHRR 41, ¶ 59 (ECtHR, 2003), https://www.5rb.com/wp-content/uploads/2013/10/Peck-v-UK-ECHR-28-Jan-03.pdf [https://perma.cc/6ZER-F3NH].

70. *Id.*

71. Antovic & Mirkovic v. Montenegro, App. No. 70838/13, ¶ 44 (Nov. 28, 2018), https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-178904%22]} [https://perma.cc/SW7H-W34Q].

is collected and stored, without his/her knowledge.[72] The Court also considers that an interference arises when electronic data is searched and seized on computer servers,[73] hard drives[74] and floppy disks.[75] In light of this, it is clear that reading someone's thoughts would qualify as an "interference." An interference would also arise under the ICCPR. In fact, in *General Comment No. 16*, the HRC describes "[t]he gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies" as interferences which "must be regulated by law."[76]

The second step of the test consists in determining whether the interference was "in accordance with the law," "unlawful" or "arbitrary." The first two criteria are not difficult to assess: they mean that interferences can only take place in cases envisaged by the law.[77] The ECtHR had the opportunity to emphasize that national law has to be clear, foreseeable, and adequately accessible.[78] In the *Shimovolos* case, specific requirements were defined regarding secret surveillance:

> The Court reiterates in this connection that in the special context of secret measures of surveillance the above requirements cannot mean that an individual should be able to foresee when the authorities are likely to resort to secret surveillance so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on the application of secret measures of surveillance, especially as the technology available for use is continually becoming more sophisticated. The law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures

---

72. Copland v. UK, 45 Eur. H.R. Rep. 37, ¶ 44 (2007), https://www.5rb.com/wp-content/uploads/2013/10/Copland-v-UK-ECHR-3-Apr-2007.pdf [https://perma.cc/N8DR-CLH8].

73. Wieser v. Austria, 46 Eur. H.R. Rep. 54, ¶ 45 (2007), https://www.legal-tools.org/doc/502dd6/pdf/ [https://perma.cc/754B-5V8L].

74. Sallinen v. Finland, 44 Eur. H.R. Rep. 18, ¶ 71 (2005), https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22CASE%20OF%20PETRI%20SALLINEN%20AND%20OTHERS%20v.%20FINLAND\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-70283%22]} [https://perma.cc/3AEZ-QAH8].

75. Stefanov v. Bulgaria, App. No. 65755/01, ¶ 42 (2006), http://hrlibrary.umn.edu/research/bulgaria/IStefanov_en.pdf [https://perma.cc/H6EK-7G6H].

76. U.N. Hum. Rts. Comm., CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation', ¶ 10 (1988), https://www.refworld.org/docid/453883f922.html [https://perma.cc/3ZJZ-CBKF].

77. *Id.* ¶ 3.

78. Silver and others v. UK, App. No. 5947/725, Eur. Ct. H. R. 347, ¶¶ 86–88 (1983); *see also* Council of Europe, Guide on Article 8 of the European Convention of Human Rights (Aug. 31, 2021), ¶ 16, https://www.echr.coe.int/Doc uments/Guide_Art_8_ENG.pdf [https://perma.cc/ZJ9F-JBGK].

> of secret surveillance and collection of data. In addition, because of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out in statute law to avoid abuses: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.[79]

This means that, if States decide to read someone's thoughts, they will not only need to pass laws which authorize them to do so. They will also have to make sure that the law is sufficiently "clear" and "detailed", in order to give citizens "an adequate indication of the conditions and circumstances" in which surveillance may be resorted to. The other conditions mentioned in *Shimovolos*—i.e., nature, scope, duration, grounds, competent authorities and remedies—shall also be mentioned in the law. The criterion of arbitrariness, which was identified by the HRC, "is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances."[80] It seems, however, that accessing someone's thoughts would not be arbitrary in all circumstances: something which will be discussed below.

The third step consists in determining if the interference was proportionate to a legitimate aim. Under Article 8(2) of the ECHR, legitimate aims consist of the "interests of national security, public safety or the economic wellbeing of the country," "prevention of disorder or crime," the "protection of health or morals," or "the protection of the rights and freedoms of others."[81] Under the ICCPR, legitimate objectives consist of "preventing the commission of further crimes" and "protecting the public,"[82] as well as the preservation of "national security, public order (order public), public health or morals or the rights and freedoms of others."[83] In *Piechowicz*, the ECtHR said that the notion of "necessity" from the term "necessary in a democratic society," means that the "interference must correspond to a pressing social need, and, in particular, must remain proportionate to the

79. Shimovolos v. Russia, Eur. Ct. H.R. 987, ¶ 68 (2011).
80. U.N. Hum. Rts. Comm. General Comment No. 16, *supra* note 76, at 1.
81. *See also* Leander v. Sweden, App. No. 9248/81, 9 Eur. H.R. Rep. 433, 452–53 (1987); *id.* at ¶ 49.
82. UN International Covenant on Civil and Political Rights, *supra* note 64, at ¶ 8.11.
83. U.N. Hum. Rts. Comm., Ilyasov v. Kazakhstan, UN Doc. CCPR/C/111/D/2009/2010, ¶ 7.7 (2014); *see also* MANFRED NOWAK, UN COVENANT ON CIVIL AND POLITICAL RIGHTS—CCPR COMMENTARY 463 (2005).

legitimate aim pursued."[84] It appears that reading a person's thoughts may well be justified by one of these legitimate aims. Organized crimes such as terrorism or trafficking are the most obvious examples. Imagine that someone who lives in State A is suspected by State B of preparing a terrorist attack. State B decides to read the suspect's thoughts. The suspicions may be confirmed, and State B would be able to take appropriate action such as arresting the suspect and their accomplices as they cross the border, or warning the authorities of State A. In this situation, reading thoughts would be justified by national security, public safety, crime prevention, and the protection of others' rights. It is certainly proportional and, to a certain extent, it may be less humiliating and stressful for the suspect than being arrested and held into custody. However, ordinary citizens would probably not be the only targets of surveillance. If politicians are equipped with BCIs, would it be lawful for a foreign nation to access their thoughts? Politicians, in their capacity as private persons, still enjoy the protection of human rights conventions.[85] However, up to now neither the ECtHR nor the HRC have decided that politicians' communications enjoyed special protection.[86] This means that reading a politician's thoughts is not contrary to the right to privacy, if the three-step test is complied with. For instance, if State A suspects that State B prepares an attack, it may be tempting to monitor the thoughts of decision-makers in State B, in the interests of national security and public safety. Accessing someone's thoughts may also be justified in more controversial situations, like the theft of trade secrets, provided that it is necessary to ensure "the economic wellbeing of the country."[87]

b. Freedom of Thought

As mentioned above, accessing someone's thought would likely not breach their privacy, in at least some circumstances. This is because Articles 8 ECHR and 17 ICCPR may be derogated from. However, things are very different with Articles 9 ECHR and 18 ICCPR. In fact, no derogation from Article 18 ICCPR may be made,[88] and Article 9 ECHR "unconditionally protects freedom of thought, conscience and religion and

84. Piechowicz v. Poland, 689 Eur. Ct. H.R., ¶ 212 (2012).

85. *See* Stefan Talmon, *Tapping the German Chancellor's Cell Phone and Public International Law*, CAMBRIDGE INT'L L.J. (Nov. 6, 2013), http://cilj.co.uk/2013/11/06/tapping-german-chancellors-cell-phone-public-international-law/ [https://perma.cc/2Q8A-KL7T].

86. On the issue of political activities *see*: Rotaru v. Romania, 192 Eur. Ct. H.R. (2000).

87. On this issue, *see* BUCHAN, *supra* note 40, at 119; THIBAULT MOULIN, CYBER-ESPIONAGE IN INTERNATIONAL LAW: SILENCE SPEAKS (2023).

88. ICCPR, *supra* note 18, art. 4.2.

enshrines a conditional right to manifest one's belief, subject to the restrictions in Article 9 § 2."[89]

If freedom of thought, conscience, and religion shall be protected, it is the same for the right *not* to express one's thought. In *General Comment No. 22*, the HRC underlined that, "[i]n accordance with Articles 18(2) and 17, no one can be compelled to reveal his thoughts or adherence to a religion or belief."[90] In *General Comment No. 34*, the Committee adopted a similar position, when it stressed out that "[a]ny form of effort to coerce the holding or not holding of any opinion is prohibited. Freedom to express one's opinion necessarily includes freedom not to express one's opinion."[91] The ECtHR agreed, and considered:

> [T]he right to manifest one's religion or beliefs also has a negative aspect, namely an individual's right not to be obliged to disclose his or her religion or beliefs and not to be obliged to act in such a way that it is possible to conclude that he or she holds—or does not hold—such beliefs.[92]

Therefore, "State authorities are not entitled to intervene in the sphere of an individual's freedom of conscience and to seek to discover his or her religious beliefs or oblige him or her to disclose such beliefs."[93] In light of the above, it appears that reading someone's thoughts would *ipso facto* result in a breach of Articles 9 and 18 ICCPR.[94] Paul Wolpe once advocated:

> The skull should be designated as a domain of absolute privacy. No one should be able to probe an individual's mind against their will. We should not permit it with a court order. We should not permit it for military or national security. We

89. Eur. Ct. H.R., *National security and European case-law*, at 22 (2013).

90. U.N. Hum. Rts. Comm., *General Comment No. 22: Article 18 (Freedom of Thought, Conscience or Religion)*, 48th Sess, adopted 30 July 1993, CCPR/C/21/Rev.1/Add.4, ¶ 3, online: https://www.equalrightstrust.org/ertdocumentbank/general%20comment%2022.pdf [https://perma.cc/982A-RCQ4].

91. U.N. Hum. Rts. Comm., *General Comment No. 34: Article 19 (Freedoms of opinion and expression)*, 102nd Sess, adopted 12 September 2011, UN Doc. CCPR/C/GC/34, ¶ 10, online: https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf [https://perma.cc/8FHE-82PB].

92. Stavropoulos and others v. Greece, App. No. 52484/18, ¶ 44 (June 25, 2020), https://hudoc.echr.coe.int/fre/#{%22itemid%22:[%22001-203165%22]} [https://perma.cc/97H4-ZXF8].

93. *Id*.

94. *See* ICCPR, *supra* note 18, at arts. 9, 18 (Mar. 23, 1976), https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights [https://perma.cc/7V34-BXLC].

> should forgo the use of the technology under coercive circumstances even though using it may serve the public good.[95]

In fact, it may be argued that it is already the case. However, the relevance of this "sacrosanctity" of the human mind may be discussed. As explained previously, accessing a person's thoughts may have advantages in certain circumstances, like the prevention of organized crime.[96]

2. Controlling Someone

Various rights and prohibitions require review when someone is subject to remote control. First, remote control (a) does not constitute torture and rarely results in inhuman treatment, but, at least under the ECHR, indeed constitutes degrading treatment. Second, remote control can hardly be described as (b) slavery, servitude, forced or compulsory labor. Third and fourth, it is (c) neither contrary to the right to liberty, or (d) the freedom of movement. Fifth, mind control (e) may sometimes breach freedom of thought.

a. The Prohibition of Torture, Cruel, Inhuman or Degrading Treatment or Punishment

Articles 3 of the ECHR and 7 of the ICCPR both prohibit torture, inhuman or degrading treatment or punishment. The only minor difference between them is that "cruel" treatment is also banned by the ICCPR. It appears that they do not only prohibit the infliction of physical pain, but also acts "that cause mental suffering to the victim."[97]

In *General Comment No. 20*, the HRC underlined that "[t]he Covenant does not contain any definition of the concepts covered by Article 7," but considered it "[un]necessary to draw up a list of prohibited acts or to establish sharp distinctions between the different kinds of punishment or treatment."[98] The Committee explained that "the distinctions depend on the nature, purpose and severity of the treatment applied."[99] The case law of the HRC, however, is not very helpful in clarifying this distinction. Some indications may nevertheless be found in *Vuolanne*:

---

95. *See* Paul Wolpe, *Is My Mind Mine?,* FORBES, (Oct. 9, 2009), https://www.forbes.com/2009/10/09/neuroimaging-neuroscience-mind-reading-opinions-contributors-paul-root-wolpe.html?sh=73fdc0cf6147 [https://perma.cc/32R6-ZXT2].

96. For a similar opinion see Andorno, *supra* note 25, at 16.

97. U.N. Hum. Rts. Comm., General Comment No. 20: Prohibition of Torture, or Other Cruel, Inhuman or Degrading Treatment or Punishment (Art. 7), ¶ 5 (1992).

98. *Id.* ¶ 4.

99. *Id*.

> The Committee . . . observes that the assessment of what constitutes inhuman or degrading treatment falling within the meaning of Article 7 depends on all the circumstances of the case, such as the duration and manner of the treatment, its physical or mental effects as well as the sex, age and state of health of the victim. A thorough examination of the present communication has not disclosed any facts in support of the author's allegations that he is a victim of a violation of his rights set forth in Article 7. In no case was severe pain or suffering, whether physical or mental, inflicted upon Antti Vuolanne by or at the instigation of a public official; nor does it appear that the solitary confinement to which the author was subjected, having regard to its strictness, duration and the end pursued, produced any adverse physical or mental effects on him. Furthermore, it has not been established that Mr. Vuolanne suffered any humiliation or that his dignity was interfered with apart from the embarrassment inherent in the disciplinary measure to which he was subjected. In this connection, the Committee expresses the view that for punishment to be degrading, the humiliation or debasement involved must exceed a particular level and must, in any event, entail other elements beyond the mere fact of deprivation of liberty.[100]

In the absence of physical pain suffered, it seems that "adverse mental effects," "humiliation" or "debasement" which "exceed a particular level" must be proven. Importantly, the "lack of consent" of the victim to a specific treatment does not result *ipso facto* in a breach of Article 7 ICCPR.[101] It means that, even if someone is remotely controlled, but does not experience physical pain, adverse mental effects or humiliation, then Article 7 is not violated.

The application of the ECHR has a different result. In the *Greek* case of 1969,[102] the Commission considered that "[t]reatment or punishment of an individual may be said to be degrading if it grossly humiliates him before others or drives him to act against his will or conscience."[103] In other words, even if treatment does not cause physical pain, adverse mental effects or humiliation, the treatment may still be contrary to Article 3 if it "drives [someone] to act against [one's] will or conscience." Yet, if an

100. U.N. Hum. Rts. Comm., Vuolanne v. Finland, UN Doc. CCPR/C/35/D/265/1987, ¶ 9.2 (Apr. 7, 1989).

101. Moulin, *supra* note 24.

102. Ireland v. United Kingdom, App. No. 5310/71 Eur. Ct. H.R., para. 162, 167 (1978) (clarifying that the distinction between these treatments 'derives principally from a difference in the intensity of the suffering inflicted and highlighting that 'ill-treatment must attain a minimum level of severity if it is to fall within the scope of Article 3', the 'assessment of this minimum' being 'relative'. The Court stated that the assessment depends on all the circumstances of the case, such as the duration of the treatment, its physical or mental effects and, in some cases, the sex, age and state of health of the victim.)

103. MARTINUS NIJHOFF, YEAR ON THE EUROPEAN CONVECTION OF HUMAN RIGHTS 186 (1972).

individual is remotely controlled, this person will *ipso facto* be driven to act against his/her conscience. This means that at the least remote control systematically results in degrading treatment. The difference between "degrading" and "inhuman" treatment was also made clear in the *Greek* case: "[t]he notion of inhuman treatment covers at least such treatment as deliberately causes severe suffering, mental or physical, which, in the particular situation, is unjustifiable."[104] If the controlled person experiences severe mental or physical suffering, but that it is only an incidental effect, then suffering is not "deliberately" caused and no inhuman treatment occurs. The outcome may be different if this person is driven to commit self-harm, as will be further discussed shortly. Finally, "[t]he word "torture" is often used to describe inhumane treatment which has a purpose, such as the obtaining of information or confessions, or the infliction of punishment, and it is generally an aggravated form of inhuman treatment."[105] The test would be hard to pass in the event of remote control, as the constituent elements of an inhuman treatment are required (i.e., the deliberate infliction of severe mental or physical suffering) as well as a specific goal (i.e., obtaining information).[106]

b. The Prohibition of Slavery, Servitude, Forced or Compulsory Labor

Articles 4 of the ECHR and 8 of the ICCPR both prohibit slavery, servitude, and forced or compulsory labor. Since a person might be driven to carry out a task while being controlled, it is of interest determine if these provisions are breached in this context.

First, it is necessary to define slavery and to consider whether the ECtHR has been breached if an individual carries out a task while being controlled. In *Siliadin*, the ECtHR developed an approach to slavery. The relevant provision is the following:

> The Court notes at the outset that, according to the 1927 Slavery Convention, "slavery is the status or condition of a person over whom any or all of the powers attaching to the right of ownership are exercised". It notes that this definition corresponds to the "classic" meaning of slavery as it was practiced for centuries. Although the applicant was, in the instant case, clearly deprived of her personal

104. *Id.*

105. *Id,* ("In addition to the severity of the treatment, there is a purposive element, as recognized in the United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment . . . which defines torture in terms of the intentional infliction of severe pain or suffering with the aim, inter alia, of obtaining information, inflicting punishment or intimidating; *see also* Ilhan v. Turkey, App. No. 22277/93 Eur. Ct. H.R., ¶ 85 (2000).

106. *See* Ioana Puscas*, La quête du soldat augmenté,* LE MONDE DIPLOMATIQUE, 3 (Sept. 2017), https://www.monde-diplomatique.fr/2017/09/PUSCAS/57875 [https://perma.cc/R779-2AT7].

> autonomy, the evidence does not suggest that she was held in slavery in the proper sense, in other words that Mr. and Mrs. B. exercised a genuine right of legal ownership over her, thus reducing her to the status of an "object".[107]

Therefore, even if a person is "clearly deprived of [one's] personal autonomy," the situation is not *ipso facto* tantamount to slavery. It is indeed necessary to prove that one "exercised a genuine right of legal ownership over" another person, "thus reducing [this person] to the status of an 'object.'" The application of the ICCPR returns similar results. As underlined by Manfred Nowak, "a definition of slavery and slave trade was avoided, although the travaux préparatoires clearly demonstrate that in contrast to servitude, they were understood in their narrow, traditional sense i.e., as destruction of one's juridical personality."[108] It results from this analysis that the remote control of someone can hardly be considered as slavery. Even if this person is deprived of personal autonomy, he/she is not automatically reduced to the status of an object and a genuine right of legal ownership is not *ipso facto* exercised.

Second, servitude must be defined. According to the ECtHR, servitude "means an obligation to provide one's services that is imposed by the use of coercion, and is to be linked with the concept of 'slavery.'"[109] Servitude consists of a "particularly serious form of denial of freedom . . . the obligation to perform certain services for others . . . [and] the obligation for the 'serf' to live on another person's property and the impossibility of altering his condition."[110] Under the ICCPR, servitude is equivalent to "slavery-like practices."[111] In fact, "the victims of slavery-like practices are not merely economically exploited; for a variety of reasons, such as drug addiction, fear of reprisals, fear of deportation, or deprivation of personal freedom, they may be totally dependent on other individuals."[112] Accordingly, the remote control of someone cannot *ipso facto* be considered as servitude. It may indeed be justified by several reasons, which are not necessarily economical in nature. For instance, a person may be controlled into bombing something or collecting intelligence. In addition, persons who live in another country and are subject to remote control are not "totally dependent on other individuals."

---

107. Siliadin v. France, 2005-VII Eur. Ct. H.R. 122.
108. Nowak, *supra* note 83, at 198.
109. Siliadin, *supra* note 107, ¶ 124.
110. *Id*. ¶ 123.
111. Nowak, *supra* note 83, at 200.
112. *Id*.

Third, focus must shift to "forced labor" and "compulsory labor." These terms were not defined by the ECHR and the ICCPR. However, recourse to International Labor Organization Convention No. 29 concerning forced or compulsory labor was often considered as a starting point by courts.[113] According to this convention, it means "all work or service which is exacted from any person under the menace of any penalty and for which the said person has not offered himself voluntarily."[114] However (and again), the remote control of someone can hardly be considered as such. Even if someone has not voluntarily offered to carry out a task, this does not mean the person is acting under the menace of a penalty.

c. The Right to Liberty

Articles 5 of the ECHR and 9 of the ICCPR both mention that "[e]veryone has the right to liberty and security of person," and that "no one shall be deprived of his liberty." Deprivation of liberty may only occur in accordance with a procedure established by law. However, where the ICCPR mentions that deprivation of liberty may occur "on such grounds . . . as are established by law,"[115] the ECHR has a more detailed content. The ECHR contemplates six grounds of justification.[116] Articles 5 of the ECHR and 9 of the ICCPR also underline that arrested persons must be "promptly informed" of the charges against them,[117] "shall be brought promptly before a judge" or an "officer authorized by law to exercise judicial power."[118] They also guarantee the right to a speedy trial,[119] and the right to compensation for persons who are victims of unlawful arrest

113. Van der Mussele v. Belgium, App. No. 8919/80, 6 Eur. H.R. Rep. ¶ 32 (1983); Graziani-Weiss v. Austria, 58 Eur. Ct. H.R. ¶ 36 (2011); Stummer v. Austria, 54 Eur. Ct. H.R. ¶ 47 (2011).

114. Graziani-Weiss v. Austria, 58 Eur. Ct. H.R. ¶ 36 (2011).

115. ICCPR, *supra* note 18, art. 9, ¶ 1.

116. Article 5 reads as follows: "(a) the lawful detention of a person after conviction by a competent court; (b) the lawful arrest or detention of a person for noncompliance with the lawful order of a court or in order to secure the fulfilment of any obligation prescribed by law; (c) the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so; (d) the detention of a minor by lawful order for the purpose of educational supervision or his lawful detention for the purpose of bringing him before the competent legal authority; (e) the lawful detention of persons for the prevention of the spreading of infectious diseases, of persons of unsound mind, alcoholics or drug addicts or vagrants; (f) the lawful arrest or detention of a person to prevent his effecting an unauthorised entry into the country or of a person against whom action is being taken with a view to deportation or extradition." ECHR, *supra* note 19, § 1, art. 5.

117. ECHR, *supra* note 19, § 1, art. 5, ¶ 2; ICCPR, *supra* note 18, art. 9, ¶ 2.

118. ECHR, *supra* note 19, § 1, art. 5, ¶ 3; ICCPR, *supra* note 18, art. 9, ¶ 3.

119. ECHR, *supra* note 19, § 1, art. 5, ¶ 4; ICCPR, *supra* note 18, art. 9 ¶ 5.

or detention.[120] The question which arises, then, is whether taking control of someone would amount to a "deprivation of liberty." At first sight, however, Articles 5 of the ECHR and 9 of the ICCPR have a restrictive meaning and fail to regulate this situation.

In *Storck v. Germany,* the ECtHR underlined that "the notion of deprivation of liberty within the meaning of Article 5 § 1 does not only comprise the objective element of a person's confinement in a particular restricted space for a not negligible length of time."[121] In fact, "[a] person can only be considered to have been deprived of his liberty if, as an additional subjective element, he has not validly consented to the confinement in question."[122] Therefore—and leaving aside the "subjective element" of consent—deprivation of liberty includes an "objective element"—i.e., "a person's confinement in a particular restricted space for a not negligible length of time."[123] It does not adapt to the situation where a person would be remotely controlled.[124] In *Ashingdane*, the ECtHR defined a test to determine if liberty deprivation occurred. The "concrete situation of the individual concerned" was described as the "starting point" and then, a range of criteria had to be taken into account, "such as the type, duration, effects and manner of implementation of the measure in question."[125] The Court also underlined that "[t]he distinction between deprivation of and restriction upon liberty is merely one of degree or intensity, and not one

120. ECHR, *supra* note 19, § 1, art. 5, ¶ 5; ICCPR, *supra* note 18, art. 9, ¶ 5.

121. Storck v. Germany, App. No. 61603/00, ¶ 74 (June 16, 2005), https://www.globalhealthrights.org/wp-content/uploads/2013/10/ECtHR-2005-Storck-v-Germany.pdf [https://perma.cc/JQJ9-Q78K].

122. *Id.*

123. COUNCIL OF EUROPE: EUROPEAN COURT OF HUMAN RIGHTS, *Guide on Article 5 of the European Convention on Human Rights – Right to Liberty and Security*, ¶ 10 (Dec. 31, 2020), https://www.refworld.org/docid/6048e29f0.html [https://perma.cc/7TAX-CTTK].

124. In the *Guide on Article 5*, the ECtHR underlined that the question of applicability of Article 5 has arisen in a variety of circumstances, including: "the placement of individuals in psychiatric or social care institutions; taking of an individual by paramedics and police officers to hospitals; confinement in airport transit zones; confinement in land border transit zones; questioning in a police station; placement in a police car to draw up an administrative-offence report; stops and searches by the police, house search; police escorting, crowd control measures adopted by the police on public order grounds; house arrest; holding sea-migrants in reception facilities and on ships; keeping irregular migrants in asylum hotspot facilities; national lockdown on account of the Covid-19 pandemic." *See id.*, ¶ 19; https://www.echr.coe.int/documents/guide_art_5_eng.pdf [https://perma.cc/FH9J-837T].

125. Ashingdane v. United Kingdom, App. No. 8225/78, ¶ 41 (May 28, 1985), https://www.stradalex.com/en/sl_src_publ_jur_int/document/echr_8225–78 [https://perma.cc/J2BK-KRWT].

of nature or substance."[126] It is interesting to note that, in *HL,* the Court applied this test, and considered "the key factor in the present case to be that the health care professionals treating and managing the applicant exercised complete and effective control over his care and movements."[127] The situation in *HL* was unique; an autistic patient, who had an history of self-harm, was detained at the hospital.[128] For the time being, the remote control of someone shall not be described as a deprivation or a restriction of liberty. However, Article 5 contains potential for regulating the remote control of an individual if this concept of "complete and effective control over movements" is considered as an autonomous test. Alternatively, it would be interesting to describe the concept of "being locked in one's own body" as an impediment to the right to liberty.

In his *CCPR Commentary*, Manfred Nowak underlined that Article 9 ICCPR had a restrictive meaning too:

> The term liberty of person is quite narrow and must not be confused with that of liberty in general. All human rights ultimately serve the realization of human freedom, even when, in accordance with their object and purpose, they may be assigned differing dimensions of liberty. Liberty of person, on the other hand, relates only to a very specific aspect of human liberty: the freedom of bodily movement in the narrowest sense. An interference with personal liberty results only from the forceful detention of a person at a certain, narrowly bounded location, such as a prison or some other detention facility, a psychiatric facility, a re-education, concentration or work camp, or a detoxification facility for alcoholics or drug addicts, as well as an order of house arrest.[129]

This conception was confirmed by *General Comment No. 35*. First, "[l]iberty of person concerns freedom from confinement of the body, not a general freedom of action."[130] Second, "[d]eprivation of personal liberty is without free consent."[131] The Committee also provided a list with examples of liberty deprivation, which all consist of physical restrictions.[132] Even if remote control is "without free consent," there is no physical confinement

---

126. *Id*.

127. HL v. United Kingdom*,* App. No. 45508/99, ¶ 91 (Jan. 5, 2005), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-66757%22]} [https://perma.cc/2KJQ-MVFN].

128. *Id.* ¶¶ 3, 9.

129. Nowak, *supra* note 83, at 212.

130. U.N. Hum. Rts. Comm., General Comment No. 35: *Article 9 (Liberty and security of person),* ¶ 3, U.N. Doc. CCPR/C/GC/35 (Dec. 16, 2014).

131. *Id.* ¶ 6.

132. Examples of deprivation of liberty include police custody, arraigo, remand detention, imprisonment after conviction, house arrest, administrative detention, involuntary hospitalization, institutional custody of children and confinement to a restricted area of an airport, as well as being involuntarily transported. They also include certain further restrictions on a person who is already detained, for example, solitary confinement or the use of physical restraining devices.

Id. ¶ 5.

in this situation and thus it does not constitute a breach of the right to liberty.

d. Freedom of Movement

Article 2 of the Fourth Protocol of the ECHR, as well as Article 12 of the ICCPR, mention that "[e]veryone lawfully within the territory of a State shall, within that territory, have the right to liberty of movement and freedom to choose his residence" and "[e]veryone shall be free to leave any country, including his own."[133] In a certain sense, one may argue that controlling an individual would impede the freedom of movement. It may be noted that, in the opinion of the HRC, "the right to reside in a place of one's choice within the territory includes protection against all forms of forced internal displacement."[134] However, it seems that the relation with a State and a foreign citizen abroad is not subject to this provision. In fact, the provision is supposed to regulate the relation with a State and "[e]veryone lawfully within the territory" of the State.[135] Therefore, a State only breaches an individual's freedom of movement if they decide to take the remote control of persons lawfully within its territory and force them to move elsewhere.

e. Freedom of Thought

At first sight, the remote control of someone does not encroach on freedom of thought. However, a study carried out at the University of California, Los Angeles revealed that religious beliefs and political ideologies may be influenced through neuromodulation.[136] It is not excluded that someone's behavior is remotely influenced, to make sure (or increase the probabilities) that they behave in a certain way.[137] However, as explained above, both the ICCPR and the ECHR result in the "sacrosanctity" of the mind. According to Article 18(2) of the ICCPR, "[n]o one shall be subject

133. COUNCIL OF EUROPE: EUROPEAN COURT OF HUMAN RIGHTS, *Guide on Article 2 of Protocol No. 4 to the European Convention on Human Rights—Freedom of Movement*, ¶ 30 (Apr. 30, 2022); ICCPR, *supra* note 18, art. 12, ¶ 1.

134. U.N. Hum. Rts. Comm., General Comment No. 27: *Article 12 (Freedom of Movement)*, ¶ 7, U.N. Doc. CCPR/C/21/Rev.1/Add.9 (Nov. 2, 1999).

135. *Id.* ¶ 4.

136. Colin Holbrook et al., *Neuromodulation of group prejudice and religious belief,* 11(3) SOC. COGNITIVE AND AFFECTIVE NEUROSCIENCE 387 (2016).

137. *See id.* at 392.

to coercion which would impair his freedom to have or to adopt a religion or belief of his choice."[138] In *General Comment No. 22*, the HRC underlined:

> Article 18.2 bars coercion that would impair the right to have or adopt a religion or belief, including the use of threat of physical force or penal sanctions to compel believers or non-believers to adhere to their religious beliefs and congregations, to recant their religion or belief or to convert. Policies or practices having the same intention or effect, such as, for example, those restricting access to education, medical care, employment or the rights guaranteed by Article 25 and other provisions of the Covenant, are similarly inconsistent with article 18.2. The same protection is enjoyed by holders of all beliefs of a non-religious nature.[139]

It may be argued, though, that "changing" the opinions and beliefs of someone—and even if they are not aware of it—would be tantamount to coercion.[140] The application of the ECHR would have similar result, as the sole "[f]reedom to manifest one's religion or beliefs" may be subject to restrictions.[141]

3. Inflicting Pain or Death

Where brain-hacking is used to kill someone, it would constitute unlawful life deprivation (a). Where it is used to cause pain, it would rarely constitute torture, but inhuman and degrading treatment may indeed occur (b).

a. The Right to Life

In 2011 and 2012, two articles revealed that insulin pumps were vulnerable to hacking. This meant hackers could gain control over the device and change the dose delivered to the patient.[142] Jerome Radcliffe—who was diagnosed with diabetes and carried out an early investigation on this issue—interestingly noted:

> I always joked around that on day some hacker was going to break into my pump, give me a dose of insulin that I didn't need, which could force my blood sugar

138. ICCPR, *supra* note 18, art. 18, ¶ 2.
139. U.N. Hum. Rts. Comm. General Comment No. 16, *supra* note 76, ¶ 5.
140. Coercion may be defined as "[c]ompulsion of a free agent by physical, moral, or economic force or threat of physical force'. Implied coercion (or undue influence) may be defined as 'the improper use of power or trust in a way that deprives a person of free will and substitutes another's objective." *See Coercion Definition*, BLACK'S LAW DICTIONARY (11th ed. 2019).
141. ECHR, *supra* note 19, § 1, art. 9, ¶ 2.
142. Jim Finkle, *Medtronic insulin pumps vulnerable to hackers*, REUTERS (Aug. 26, 2011), https://www.reuters.com/article/medtronic-security-idUSN1E77O1VJ20110826 [https://perma.cc/CMC4-EF4Z].

> too low and result and render me unconscious after an hour . . . If left untreated, hypoglycemia can lead to coma and, in extreme cases, death.[143]

Unfortunately, he discovered that risk was real.[144] At the same time, another study revealed pacemakers could also be hacked. Barnaby Jack declared, "[w]ith a max voltage of 830 volts, it is not hard to see why this is a fairly deadly feature. Not only could you induce cardiac arrest, but you could continually recharge the device and deliver shocks on loop."[145] Due to the proximity with the brain, the remote hacking of a neural device may have nefarious effects.

The right to life is protected by Articles 2 of the ECHR and 6 of the ICCPR. If both preserve the possibility to impose the death penalty, the latter is subject to several conditions. Furthermore, Article 6 of the ICCPR mentions that "[n]o one shall be arbitrarily deprived of his life,"[146] and Article 2(2) of the ECHR reads as follows:

> Deprivation of life shall not be regarded as inflicted in contravention of this Article when it results from the use of force which is no more than absolutely necessary: (a) in defense of any person from unlawful violence; (b) in order to effect a lawful arrest or to prevent the escape of a person lawfully detained; (c) in action lawfully taken for the purpose of quelling a riot or insurrection.[147]

The ECtHR underlined that Article 2 is "not concerned exclusively with intentional killing,"[148] and that "the force used must be strictly proportionate to the achievement of the aim" mentioned in subparagraphs (a), (b), and (c).[149] The Court also considered that"the legitimate aim of effecting a lawful arrest can only justify putting human life at risk in circumstances of absolute necessity" and that—in principle—no such necessity exists "where it is known that the person to be arrested poses no threat to life or limb and is not suspected of having committed a violent offence, even if

143. Jerome Radcliffe, Address at Black Hat USA 2011, *Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System* (Aug. 4, 2011) (transcript available at https://cs.uno.edu/~dbilar/BH-US-2011/materials/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf [https://perma.cc/S8PY-658J]).

144. *Id.*

145. Darren Pauli, *Hacked terminals capable of causing pacemaker deaths*, IT NEWS, Oct. 17, 2012, https://www.itnews.com.au/news/hacked-terminals-capable-of-causing-pacemaker-mass-murder-319508 [https://perma.cc/G84U-RVCN].

146. ICCPR, *supra* note 18, art. 6, ¶ 1.

147. ECHR, *supra* note 19, § 1, art. 2, ¶¶ 1–2.

148. McCann v. United Kingdom, App. No. 18984/91, ¶ 148 (Sept. 27, 1995), https://hudoc.echr.coe.int/eng?i=001-57943 [https://perma.cc/LTC2-Q843].

149. *Id.* ¶ 149.

a failure to use lethal force may result in the opportunity to arrest the fugitive being lost."[150] Then, a law enforcement operation must "be planned and controlled so as to minimize to the greatest extent possible recourse to lethal force or incidental loss of life."[151] The Court also considered that "it cannot substitute its own assessment of the situation for that of an officer who was required to react in the heat of the moment to avert an honestly perceived danger to his life."[152] In addition, the responsibility of the State may be engaged where agents "fail to take all feasible precautions in the choice of means and methods of a security operation mounted against an opposing group with a view to avoiding and, in any event, to minimizing incidental loss of civilian life."[153] When someone died in circumstances outside the exceptions of Article 2, the ECtHR considers that an extra-judicial killing occurred and therefore, a breach of the right to life.[154] It may be noted that the ECtHR described a policy of Eastern Germany—which consisted in "annihilat[ing] border violators and protect the border at all costs"—as a breach of Article 2.[155]

The HRC clarified the notion of "arbitrariness" in the context of Article 6 of the ICCPR. In *General Comment No. 36*, the Committee underlined:

> The use of potentially lethal force for law enforcement purposes is an extreme measure, which should be resorted to only when strictly necessary in order to protect life or prevent serious injury from an imminent threat. It cannot be used, for example, in order to prevent the escape from custody of a suspected criminal or a convict who does not pose a serious and imminent threat to the lives or bodily integrity of others. The intentional taking of life by any means is permissible only if it is strictly necessary in order to protect life from an imminent threat.[156]

It results from the above that the remote killing of someone is subject to strict conditions. Under the ECHR and the ICCPR, lethal force may only be used to prevent threat to life or limb, to arrest someone who poses such threat, and under the ECHR, to quell a riot or an insurrection. These conditions may be met in certain circumstances. For example, if someone is planning

---

150. Nachova and Others v. Bulgaria, App. No. 43577/98, ¶ 95 (July 6, 2005), https://hudoc.echr.coe.int/eng?i=001-69630 [https://perma.cc/3Q96-5Q9H].

151. Bubbins v. United Kingdom, App. No. 50196/99, ¶ 136 (June 17, 2005), https://hudoc.echr.coe.int/eng?i=001-68548 [https://perma.cc/B58V-JXK2].

152. *Id.* ¶ 139.

153. Özkan v. Turkey, App. No. 21689/93, ¶ 297 (Apr. 6, 2004), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-61696%22]} [https://perma.cc/NVG4-3YVN].

154. *See* COUNCIL OF EUROPE: EUROPEAN COURT OF HUMAN RIGHTS, *Guide on Article 2 of the European Convention on Human Rights—Right to life*, ¶ 119 (Dec. 31, 2021), https://www.refworld.org/docid/6048e29c2.html [https://perma.cc/AP5S-FCCT].

155. Streletz, Kessler and Krenz v. Germany, 2001-II Eur. Ct. H.R. 409, 449–50 (2001).

156. U.N. Hum. Rts. Comm., General Comment No. 36: *Article 6 (Right to Life)*, ¶ 12, CCPR/C/GC/36 (Sept. 30, 2019).

an attack, or is at large and constitutes a danger, then this person may be hacked and neutralized. It is also conceivable that law-enforcement officers, who are investigating a case, could discover that they are being hacked. In this scenario, if the officers fear for their lives, it would be admissible for them to hack back. In these situations–and provided that it was strictly necessary–Articles 2 of the ECHR and 6 of the ICCPR would not be breached.

b. The Prohibition of Torture, Cruel, Inhuman or Degrading Treatment

A study conducted in Oxford revealed that "the increasing sophistication of invasive neuromodulation, coupled with developments in information security research and consumer electronics, has resulted in a small but real risk of malicious individuals accessing implantable pulse generators (IPGs)."[157] This means that "[u]nauthorized access to IPGs could cause serious harm to the patients in whom the devices are implanted."[158] The same study underlined that it was feasible to alter motor function,[159] provoke pain,[160] alter impulse control,[161] or modify emotion and affect.[162] As previously explained, Articles 3 of the ECHR and 7 of the ICCPR are relevant in this context. A breach of these provisions may occur in the event of physical pain, adverse mental effects, humiliation or debasement which exceed a particular level.

First, one may argue this type of hacking does not constitute torture. Even though severe mental or physical suffering may be deliberately inflicted in this situation, it does not seem that a specific goal—such as obtaining information, confessions, or inflicting punishment—does exist. This interpretation is confirmed by the definition of "torture" in the United Nations Convention Against Torture (UNCAT):

> For the purposes of this Convention, the term "torture" means any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering

157. Pycroft, *supra* note 17, at 454.
158. *Id*.
159. *Id.* at 456.
160. *Id*.
161. *Id*, at 457.
162. *Id*.

> is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity. It does not include pain or suffering arising only from, inherent in or incidental to lawful sanctions.[163]

Second, brain-hacking may constitute inhuman treatment. In the *Greek* case, the ECtHR affirmed that the "notion of inhuman treatment covers at least such treatment as deliberately caus[ing] severe suffering, mental or physical, which, in the particular situation, is unjustifiable."[164] This notion of "justifiability" was controversial. In fact, it "applies only to the assessment of individual facts in the particular context in which they occur and not to the determination of a violation of Article 3 as such."[165] Hence, "[j]ustifiability is a yardstick for assessing the weight to be attached to factors such as the nature of the victim and the circumstances in which the ill-treatment is said to have arisen."[166] According to the HRC, "the distinctions [between torture, inhuman or degrading treatment] depend on the nature, purpose and severity of the treatment applied."[167] In the type of hacking contemplated here, the infliction of gratuitous suffering could be deliberate, and severe mental or physical suffering may indeed occur.[168] For example, if hacking results in excessive paranoia, feelings of persecution, hallucinations, or serious depression it could be defined as inhuman treatment.

Third, brain-hacking may constitute degrading treatment. Degrading treatment occurs where someone is subject to humiliation or debasement beyond a particular level,[169] gross humiliation, or is being driven to act against one's will or conscience.[170] It is particularly relevant if hacking is used to alter impulse control. According to an early study carried out by American and Spanish researchers between 1999 and 2000, brain stimulation could result in "euphoria," "showed logorrhea with press of speech," "overactivity," "grandiose delusions," "increased sexual drive," and

---

163. Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, art. 1, ¶ 1, Dec. 10, 1984, 1465 U.N.T.S. 85.

164. NIJHOFF, *supra* note 103.

165. Michael K. Addo & Nicholas Grief, *Does Article 3 of The European Convention on Human Rights Enshrine Absolute Rights?*, 9 EUR. J. INT'L L. 510, 522 (1998).

166. *Id.*

167. U.N. Hum. Rts. Comm. General Comment No. 20, *supra* note 97, ¶ 4.

168. In a medical context, it appears that "[p]ain is a subjective symptom that is difficult for health care professionals to evaluate and characterize." Therefore, "it is important to respect patients' own assessments when they are able to communicate or, alternatively, a properly qualified health care professional's assessment of noncommunicating patients." *See* Ana Rita Pais de Queiróz Pinheiro & Rita Margarida Dourado Marques, *Behavioral Pain Scale and Critical Care Pain Observation Tool for pain evaluation in orotracheally tubed critical patients. A systematic review of the literature*, 31(4) REV. BRAS. TER. INTENSIVA 571, 571 (2019).

169. Vuolanne, *supra* note 100.

170. NIJHOFF, *supra* note 103.

"inappropriate sexual behavior."[171] A degrading treatment could arise if hacking has such effect, and that the subject behaves in a way which is particularly humiliating–for instance if the subject becomes ridiculous, is incontinent, makes verbal or behavioral sexual advances, or spends all of their money.

C. The Positive Obligations of a State Party Against Brain-Hacking

According to the analysis above, jurisdiction cannot be exercised abroad in situations where a State remotely reads someone's thoughts, controls this person, or inflicts pain or death. This does not mean, however, that Contracting Parties are exempted from positive obligations–i.e., to protect the rights of persons within one's own territory. In *General Comment No. 31*, the HRC underlined that obligations of State Parties "will only be fully discharged if individuals are protected . . . against acts committed by private persons or entities that would impair the enjoyment of Covenant rights in so far as they are amenable to application between private persons or entities."[172] In such circumstances, State Parties breach the ICCPR if they permit, fail to take appropriate measures, or do not exercise due diligence "to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities."[173] Similar obligations arise under the ECHR. The fact threats originate from abroad do not seem to matter here. In fact, their effects would still "materialize" on the territory of a State Party (1), and recommendations will be given as to how positive obligations may be discharged vis-à-vis brain-hacking (2).

1. Relevant Positive Obligations

In the present context, relevant positive obligations would stem from the right to life (a), the prohibition of torture or cruel, inhuman or degrading treatment or punishment (b), the prohibition of slavery, servitude, forced or compulsory labor (c), the right to privacy (d), and freedom of thought (e).

171. Jaime Kulisevsky et al., *Mania following deep brain stimulation for Parkinson's disease*, 59 NEUROLOGY 1421 (2002).
172. Moulin, *supra* note 37, ¶ 8.
173. *Id.*

a. The Right to Life

In *General Comment No. 36*, the HRC underlined that "States parties must take appropriate measures to protect individuals against deprivation of life by other States, international organizations and foreign corporations operating within their territory or in other areas subject to their jurisdiction."[174] It might be said that where someone's BCI is hacked from abroad, the hacker is not acting "within" the territory of a State Party. However, if the person who is subject to hacking is within the territory of a State Party, the effects would still materialize there. In the case of *LCB*, the ECtHR "consider[ed] that the first sentence of Article 2 § 1 enjoins the State not only to refrain from the intentional and unlawful taking of life, but also to take appropriate steps to safeguard the lives of those within its jurisdiction."[175] In *Gongadze*, the Court reiterated this and explained:

> This involves a primary duty on the State to secure the right to life by putting in place effective criminal-law provisions to deter the commission of offences against the person, backed up by law enforcement machinery for the prevention, suppression and punishment of breaches of such provisions. It also extends, in appropriate circumstances, to a positive obligation on the authorities to take preventive operational measures to protect an individual or individuals whose lives are at risk from the criminal acts of another individual.[176]

However, due to "the difficulties in policing modern societies, the unpredictability of human conduct and the operational choices which must be made in terms of priorities and resources," this positive obligation "must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities."[177] The positive obligations under the right to life also consist of proper criminal investigation, procedure, and justice.

---

174. U.N. Hum. Rts. Comm. General Comment No. 36, *supra* note 156, ¶ 22.

175. Enukidze and Girgvliani v. Georgia, App. No. 25091/07, ¶¶ 242–43 (Apr. 26, 2011), https://hudoc.echr.coe.int/eng?i=001-104636 [https://perma.cc/D6TB-3GVA].

176. Gongadze v. Ukraine, App. No. 34056/02, ¶ 164 (Nov. 8, 2005), https://hudoc.echr.coe.int/fre?i=001-70853 [https://perma.cc/TA3R-94WP].

177. *Id.* ¶ 165 ("[a]ccordingly, not every claimed risk to life can entail for the authorities a Convention requirement to take operational measures to prevent that risk from materializing. For a positive obligation to arise, it must be established that the authorities knew or ought to have known at the time of the existence of a real and immediate risk to the life of an identified individual or individuals from the criminal acts of a third party, and that they failed to take measures within the scope of their powers which, judged reasonably, might have been expected to avoid that risk" citing *Kiliç v. Turkey*, no. 22492/93, §§ 62–63, ECHR 2000-III).

b. The Prohibition of Torture or Cruel, Inhuman or Degrading Treatment or Punishment

In *General Comment No. 20*, the HRC underlined that "[i]t is the duty of the State Party to afford everyone protection through legislative and other measures as may be necessary against the acts prohibited by Article 7, whether inflicted by people acting in their official capacity, outside their official capacity or in a private capacity."[178] As to the ECtHR, the Court "does not rule out the possibility that Article 3 of the Convention may also apply where the danger emanates from persons or groups of persons who are not public officials."[179] However, it must be shown "that the risk is real and that the authorities of the receiving State are not able to obviate the risk by providing appropriate protection."[180]

c. The Prohibition of Slavery, Servitude, Forced or Compulsory Labor

The HRC indicates that States must take steps to prevent and punish the exploitation of human beings. States must make sure measures are adopted and implemented in practice,[181] offences are investigated, perpetrators are tried and punished, and victims have access to appropriate protection and assistance.[182] In addition, proper legislation must be adopted and victims are entitled to reparation.[183] In the event of trafficking, States are expected to establish clear procedures for identifying victims and give sufficient

178. U.N. Hum. Rts. Comm. General Comment No. 20, *supra* note 97, ¶ 2.

179. HLR v. France, 26 EHRR 29, App. No. 24573/94, Eur. Comm'n H.R. Dec. & Rep. ¶ 40 (1997); *see also* A v. UK, App. No. 100/1997/884/1096, Eur. Comm'n H.R. Dec. & Rep. para. 22 (1998) quoting "[t]he Court considers that the obligation on the High Contracting Parties under Article 1 of the Convention to secure to everyone within their jurisdiction the rights and freedoms defined in the Convention, taken together with Article jurisdiction are not subjected to torture or inhuman 3, requires States to take measures designed to ensure that individuals within their or degrading treatment or punishment, including such ill-treatment administered by private individuals."

180. HLR v. France, 26 EHRR 29, App. No. 24573/94, Eur. Comm'n H.R. Dec. & Rep. ¶ 40 (1997).

181. *See* U.N. Hum. Rts. Comm. (concluding observations on the sixth periodic report of the Dominican Republic, U.N. Docs. CCPR/C/DOM/CO/6, ¶ 20 (2017).

182. *Id*.

183. *See* U.N. Hum. Rts. Comm. (concluding observations on the second periodic report of Honduras) U.N. Docs. CCPR/C/HND/CO/2, ¶ 37 (2017).

training to officers.[184] Inspection measures may also be required.[185] The ECtHR similarly underlined that States are expected "to adopt criminal-law provisions which penalize the practices referred to in Article 4 and to apply them in practice."[186] In addition, "[i]n order to comply with this obligation, member States are required to put in place a legislative and administrative framework to prohibit and punish trafficking."[187]

d. Right to Privacy

In *General Comment No. 16*, the HRC highlighted the obligations imposed by Article 17 "require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right."[188] The HRC also pointed out that it is precisely in State legislation above all that provisions must be made for the protection of the right set forth in that article, and it demonstrated concern that insufficient attention was given to "the manner in which respect for this right is guaranteed by legislative, administrative or judicial authorities, and in general by the competent organs."[189] The ECtHR previously underlined that, even if the essential object of Article 8 of the ECHR consists in protecting individuals "against arbitrary interference by public authorities," it may also "impose certain positive obligations to ensure effective respect for the rights protected by Article 8."[190] However, the appropriate means of actions fall within States' margin of appreciation, and "[t]here are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is in issue."[191] Yet, "[w]here a particularly important facet of an individual's existence or identity is at stake, or where the activities at stake involve a most intimate aspect of private life, the margin allowed to the State is correspondingly narrowed."[192] The measures

184. U.N. Hum. Rts. Comm. (concluding observations on the sixth periodic report of Italy) UN Doc. CCPR/C/ITA/CO/6, ¶ 29 (2017).

185. U.N. Hum. Rts. Comm. (concluding observations on the sixth periodic report of the Dominican Republic) CCPR/C/DOM/CO/6, ¶ 20 (2017).

186. Siliadin, *supra* note 107, para. 89.

187. Rantsev v. Cyprus and Russia, App. No. 25965/04, ¶ 284 (July 1, 2010), https://hudoc.echr.coe.int/fre?i=002-1142 [https://perma.cc/76UA-DVKZ].

188. U.N. Hum. Rts. Comm. General Comment No. 16, *supra* note 76, ¶ 1.

189. *Id.* ¶ 2.

190. Bărbulescu v. Romania, App. No. 61496/08, ¶ 108 (Sept. 5, 2017), https://hudoc.echr.coe.int/fre?i=001-177082 [https://perma.cc/W779-2WCD].

191. Söderman v. Sweden, App. No. 5786/08, ¶ 79 (Nov. 12, 2013), https://hudoc.echr.coe.int/eng?i=001-128043 [https://perma.cc/49RT-6VK2].

192. *Id.*; *see also* Mosley v. UK, App. No. 48009/08, ¶ 109 (Sept. 9, 2011), https://hudoc.echr.coe.int/fre?i=001-104712 [https://perma.cc/NB8T-7SBY].

adopted by the State may consist, for example, in the adoption of a legal framework,[193] the availability of a remedy enabling the actual offender to be identified and brought to justice,[194] or civil-law remedies capable of affording sufficient protection.[195]

e. Freedom of Thought

Case law about the positive obligations of States under Article 9 of the ECHR and 18 of the ICCPR usually focuses on the freedom to manifest one's opinion or religion, rather than freedom of thought. However, in *Osmanoğlu and Kocabaş*, the ECtHR mentioned that:

> The positive obligations may involve the provision of an effective and accessible means of protecting the rights guaranteed under that provision, including both the provision of a regulatory framework of adjudicatory and enforcement machinery protecting individuals' rights and the implementation, where appropriate, of specific steps . . . In that case, the Court held that there had been an obligation on the authorities to provide the applicant with an effective and accessible procedure that would have enabled him to have established whether he was entitled to conscientious objector status.[196]

2. Application to Brain-Hacking

Positive obligations of State Parties may be conceptualized as an obligation of conduct, rather than an obligation of result. States have to take appropriate measures, provide protection, adapt the legislation, and create remedies and procedures to prevent interference with the rights of persons within their territories or jurisdiction. In a cybernetical age, different measures may be expected from States.

First, if BCIs are available off-the-shelf (or even through medical prescription), States may be expected to impose security measures on moral persons (like manufacturers and providers) as well as physical persons

193. Bărbulescu v. Romania, App. No. 61496/08, ¶ 115 (Sept. 5, 2017), https://hudoc.echr.coe.int/fre?i=001-177082 (The Court identified six criteria which were relevant where the correspondence of employees was monitored by employers).

194. *See* K.U. v. Finland, App. No. 2872/02, ¶ 47 (Dec. 2, 2008), https://hudoc.echr.coe.int/fre?i=001-89964 [https://perma.cc/L6SV-U84C].

195. Noveski v. the former Yugoslav Republic of Macedonia, Apps. No.'s 25163/08, 2681/10 and 71872/13, ¶ 61 (Sept. 16, 2016), https://hudoc.echr.coe.int/eng?i=001-167505 [https://perma.cc/SVK6-NPEK].

196. Osmanoğlu and Kocabaş v. Switzerland, App. No. 29086/12, ¶ 86 (Jan. 10, 2017), https://hudoc.echr.coe.int/eng?i=001-178808 [https://perma.cc/L8EL-LK64].

(like users and third persons). The former may be required to ensure the product is free of defects, establish a 24/7 helpline, reflect on emergency procedures, and–if they have suspicions that someone is being hacked–warn the competent authorities to take action. If scientific progress reveals it is possible to remotely "switch off" BCIs without too much risk then this option may be contemplated, at least for non-therapeutic devices . A "duty of assistance" may also be defined. For instance, if someone notices that another person is being hacked, it would be made compulsory to warn the competent authorities and/or to call the emergency units.

Second, States would need to ensure that military or police units are trained to deal with this type of hacking, and—even if few indictments of foreign hackers have been successful so far—they may be required to adjust criminal law and procedure, and make extradition requests. States may even agree to amend the provisions of the Cybercrime Convention, in which they pledged to criminalize various behaviors–like illegal access, illegal interception, data interference, system interference, misuse of devices—to address brain-hacking.[197] Another problem resides in the supply chain—i.e., "the entire process of making and selling commercial goods, including every stage from the supply of materials and the manufacture of the goods through to their distribution and sale."[198] In fact, a malicious code or component may be inserted into a trusted piece of software or hardware at any step of the supply chain.[199] For instance, China was suspected of inserting chips on hardware manufactured in its territory, and the United States was suspected of opening packages to similarly insert chips.[200] A team of researchers at the University of Michigan demonstrated that the alteration of a single microchip cell—out of hundreds of millions—was sufficient to create a backdoor.[201] This backdoor enables foreign intelligence agencies and criminals to easily take control of a device. A similar scenario may occur when BCIs are subject to large-scale production, as the manufacturing plants and the users of BCIs may be based in different countries. Consequences would be dramatic if foreign governments and criminals

197. Convention on Cybercrime, ch. 2, § 1, arts. 2–6, Nov. 23, 2001, E.T.S. No. 185; *see also* Mark Gasson & Bert-Jaap Koops, Attacking *Human Implants: A New Generation of Cybercrime*, 5 L., INNOVATION AND TECH. (2), 248, 250 (2013).

198. *Supply Chain*, COLLINS DICTIONARY, https://www.collinsdictionary.com/dictionary/english/supply-chain [https://perma.cc/DG5H-LGX5] (last visited Aug. 27, 2022).

199. Andy Greenburg, *Hacker Lexicon: What Is a Supply Chain Attack?*, WIRED (May 31, 2021, 7:00 AM), https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/ [https://perma.cc/VM68-GALG].

200. THIBAULT MOULIN, LE CYBER-ESPIONNAGE EN DROIT INTERNATIONAL 26–27 (2021).

201. Andy Greenberg, *This 'Demonically Clever' Backdoor Hides In a Tiny Slice of a Computer Chip*, WIRED (June 1, 2016, 7:00 AM), https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/ [https://perma.cc/S42F-W8RF].

could access neural devices and interfere with the brains of ordinary citizens. However, solutions may exist. The researchers in Ann Arbor suggested, for instance, that a trusted component may be inserted in modern chips to ensure that programs have not been granted inappropriate operating-system-level privileges.[202] If technical solutions are available, then the legislation may be amended and further obligations may be imposed on providers who import and sell neural devices in national markets to ensure that products are delivered with an adequate level of protection. Assuming that hacking occurs and results in damage, States may be expected to adapt the legislation to ensure proper reparations–e.g., in terms of insurance policy.

III. THE POTENTIAL REGULATION OF SOME FORMS OF BRAIN-HACKING BY INTERNATIONAL HUMANITARIAN LAW

Before analyzing IHL, it is worth insisting that the application of IHRL does not stop when a conflict starts. In peacetime, provisions may be derogated from under appropriate circumstances, such is the case for Articles 8, 9(2), 10, 11 of the ECHR, and Articles 11, 19(2), 22, 25 of the ICCPR.[203] In time of war or other emergency, further derogations are permissible. However, some provisions may never be subject to restrictions: Articles 2–except in respect of deaths resulting from lawful acts of war–3, 4(1), and 7 of the ECHR,[204] and Articles 6, 7, 8 (paragraphs 1 and 2), 11, 15, 16, and 18 of the ICCPR.[205] In addition, the occupying Power is expected to comply with its human rights obligations–as "situations of military occupation appear to be a prime example in which the "effective control over an area" test is satisfied."[206] Reading thoughts would probably not be prohibited by IHL (A). In contrast, controlling someone may be contrary to the laws of war (B), and it would be the same if pain or death is inflicted (C).

202. *Id.*
203. ECHR, s*upra note* 19, arts. 8–11; ICCPR, *supra note* 18, arts. 11, 19, 22, 25.
204. ECHR, s*upra note* 19, arts. 3–4, 7.
205. ICCPR, *supra note* 18, arts. 6–8, 11, 15–16, 18.
206. Noam Lubell, *Human Rights Obligations in Military Occupation,* 94 INT'L. REV. RED Cross 317, 320 (2012).

A. Reading Thoughts

Geneva Conventions III and IV both underline that "[n]o physical or mental torture, nor any other form of coercion" may be exercised against prisoners of war and civilians to obtain information.[207] The term "coercion" means "[c]ompulsion of a free agent by physical, moral, or economic force or threat of physical force."[208] This does not correspond, however, to what happens when someone's thoughts are read.[209]

If IHL incorporates provisions about the definition and the treatment of spies–those who collect intelligence–then there is nothing about the rights of persons being spied on.[210] This body of law, so it seems, has little to say about reading thoughts *per se.* However, as mentioned above, IHRL remains relevant. It is worth underlining that, even if the right to privacy may be derogated from in time of public emergency, this is not the case for freedom of thought. The HRC, in *General Comment No. 34*, made clear that:

> [A]lthough freedom of opinion is not listed among those rights that may not be derogated from pursuant to the provisions of Article 4 of the Covenant, it is recalled that, "in those provisions of the Covenant that are not listed in Article 4, paragraph 2, there are elements that in the Committee's opinion cannot be made subject to lawful derogation under Article 4". Freedom of opinion is one such element, since it can never become necessary to derogate from it during a state of emergency.[211]

This excerpt means that, even if IHL is silent regarding access to someone's thoughts, this practice would still be prohibited by IHRL.

B. Controlling Someone

Civilians and persons who are *hors-de-combat* shall not be used as human shields. Indeed, "[t]he presence of a protected person may not be

---

207. Geneva Convention III, *supra* note 20, art. 17; Geneva Convention IV, *supra* note 20, art. 31.

208. *Coercion*, BLACK'S LAW DICTIONARY (11th ed. 2019).

209. *Compare* Dinniss & Kleffner, *supra* note 23, at 447 ("[E]nhancing a prisoner's trust in his or her captors, by, for example, increasing their levels of oxytocin, a hormone tied to social bonding and sometimes referred to as the 'cuddle hormone,' would fall afoul of the sweeping and categorical prohibition of coercion").

210. Convention (II) with Respect to the Laws and Customs of War on Land & Annex, Regulations Concerning the Laws and Customs of War on Land, art. 29, Jul. 29, 1899, 32 Stat. 1803, T.S. 403; Convention (IV) with Respect to the Laws and Customs of War on Land & Annex, Regulations Concerning the Laws and Customs of War on Land, art. 29, Oct. 18, 1907, 36 Stat. 2277, T.S. 277; Additional Protocol I, *supra* note 21, art. 46.

211. U.N. Hum. Rts. Comm. General Comment No. 34, *supra* note 91, para. 5.

used to render certain points or areas immune from military operations."[212] In addition, "[n]o prisoner of war may at any time be sent to, or detained in areas where he may be exposed to the fire of the combat zone."[213] It follows that a breach of IHL occurs if these persons are remotely controlled to be placed in "danger zones."

The Geneva Conventions also include provisions about the working conditions of these persons and draws a distinction between civilians and prisoners of wars. Civilians "may be compelled to work only to the same extent as nationals of the Party to the conflict in whose territory they are" and–if they are of enemy nationality—"they may only be compelled to do work which is normally necessary to ensure the feeding, sheltering, clothing, transport and health of human beings and which is not directly related to the conduct of military operations."[214] In addition, they may not be compelled to serve in the "armed or auxiliary forces' of the Occupying Power."[215] In contrast, prisoners of war may be subject to forced labor, but only in some fields: camp administration, installation or maintenance, agriculture, mining, manufacturing industries, public works, transport, commercial business, arts and crafts, and domestic and public utility services.[216] In particular, they shall not be expected to take part in activities that have a military purpose or that are unhealthy or dangerous.[217] The question which arises, then, is whether someone is "compelled" into doing something when they are remotely controlled. To compel means "[t]o cause or bring about by force, threats, or overwhelming pressure."[218] It is not unreasonable to equate remote control with an "overwhelming pressure" and to consider that these provisions are breached if it occurs.

212. Geneva Convention III, *supra* note 20, art. 23; Geneva Convention IV, *supra* note 20, art. 28.
213. Geneva Convention III, *supra* note 20, art. 23.
214. Geneva Convention IV, *supra* note 20, art. 40 (In addition, they "shall have the benefit of the same working conditions and of the same safeguards as national workers, in particular as regards wages, hours of labor, clothing and equipment, previous training and compensation for occupational accidents and diseases.").
215. *Id.* art. 51.
216. *See* Geneva Convention III, *supra* note 20, arts. 49–50.
217. *See id.* art. 52.
218. *Compel*, BLACK'S LAW DICTIONARY (11th ed. 2019).

C. *Inflicting Pain or Death*

The Geneva Convention specifies that civilians and persons who are *hors-de-combat* are provided specific protections. They shall not be subject to violence, acts, or omissions which may endanger their lives or health, mutilation, and medical or scientific experimentation.[219] Further, they shall not be taken as hostages.[220] Such prohibition also applies "in the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties," and "shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons."[221]

Several provisions in the First Additional Protocol to the Geneva Conventions aim at protecting civilians during hostilities. According to the principle of distinction, "[i]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[222] In addition, civilian populations and civilians "shall not be the object of attack" and shall not be subject to "acts or threats of violence the primary purpose of which is to spread terror among the civilian population."[223] Indiscriminate attacks are also prohibited and are defined as "those which are not directed at a specific military objective,"[224] "those which employ a method or means of combat which cannot be directed at a specific military objective,"[225] and "those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol."[226]

It is important to recognize that the provisions of the Geneva Conventions III and IV "shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."[227] In addition, "[t]he provisions of [Additional Protocol I] with respect to attacks

---

219. Geneva Convention III, *supra* note 20, art. 13; Geneva Convention IV, *supra* note 20, art. 32.
220. Geneva Convention III, *supra* note 20, art. 3; Geneva Convention IV, *supra* note 20, art. 34.
221. Geneva Convention III, *supra* note 20, art. 3; Geneva Convention IV, *supra* note 20, art. 3.
222. Additional Protocol I, *supra* note 21, art. 48.
223. *Id.* art. 51(2).
224. *Id.* art. 51(4)(a).
225. *Id.* art. 51(4)(b).
226. *Id.* art. 51(4)(c).
227. Geneva Convention III, *supra* note 20, art. 2; Geneva Convention IV, *supra* note 20, art. 2.

apply to all attacks in whatever territory conducted, including the national territory belonging to a Party to the conflict but under the control of an adverse Party."[228]

The above illustrates that acts of violence exclusively directed at protected persons are prohibited. It would be forbidden, under the laws of war, to remotely kill, inflict physical or mental pain to them. To threaten to do so in order to gain an advantage would also be prohibited. This would indeed correspond to the definition of hostage-taking—i.e., "[t]he unlawful holding of an unwilling person as security that the holder's terms will be met by an adversary."[229] In addition, the fear of being hacked is the kind of act which may (illegally) spread terror among civilian population.

The investigations conducted by Barnaby Jack about pacemakers, revealed that it was possible to access the manufacturer's development server and that "data could be used be used to load rogue firmware which could spread between pacemakers" with "the potential to commit mass murder."[230] He also declared: "[t]he worst case scenario that I can think of, which is 100 percent possible with these devices, would be to load a compromised firmware update onto a programmer and . . . the compromised programmer would then infect the next pacemaker or ICD and then each would subsequently infect all others in range."[231] A similar scenario is conceivable with BCIs. Even if a belligerent party is not intending to kill civilians in particular, it may decide to infect neural devices in a way which may equally kill enemy soldiers and civilians. This would result in a violation of the laws of war, as this type of hacking would be considered "a method or means of combat which cannot be directed at a specific military objective."[232] In addition, and even if a means or method of warfare may be directed at military objectives, the following shall be considered as indiscriminate and therefore, forbidden by IHL: an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated. In contrast, it means that "incidental loss of civilian life" which is not excessive in relation to the "concrete and direct military advantage anticipated" would not be a violation of the laws of war. For instance, let's say that members

228. Additional Protocol I, *supra* note 21, art. 49(2).
229. *Hostage-Taking*, BLACK'S LAW DICTIONARY (11th ed. 2019).
230. Pauli, *supra* note 145.
231. *Id*.
232. Additional Protocol I, *supra* note 21, art. 51(4)(b)

of the armed forces are equipped with a specific type of neurotechnology and that, for some reason, civilians have similar devices. It would be acceptable to describe them as part of "collateral damage" if a remote attack enables a belligerent Party to secure a military advantage but kills them—as long as proportionality is respected.

IV. CONCLUSION

Woodrow Barfield and Alexander Williams once underlined that "for reasons of ensuring freedom of the mind in the coming cyborg age, it is imperative that the human body and mind be considered sacrosanct; to invade a person's mind without their consent should be an egregious human rights violation."[233] In fact, existing rules of IHRL are not entirely toothless vis-à-vis brain-hacking, and–even if some experts advocated the contrary–the creation of a new body of "mental privacy" is not necessarily required.[234] For instance, freedom of thought (Articles 9(1) of the ECHR and 18(1) of the ICCPR) is very protective and prevents States from reading someone's thoughts.[235] However, the relevance of the "sacrosanctity" of the mind may be discussed. For instance, the necessity to prevent an imminent crime is a situation where it would be reasonable to read someone's thoughts. In addition, some situations of remote control and modulation would constitute a breach of this freedom. If Article 3 ECHR satisfactorily regulates situations of remote control, it is not the same for Article 7 ICCPR. In fact, it would be a good thing if the interpretation of "degrading treatment" under the ICCPR was similar to the conception promoted by the ECHR—i.e., that such degrading treatment occurs as soon as someone is driven to act against their conscience, and even if this person does not feel physical or mental pain. Another disappointing finding is the irrelevance—in the event of remote control–of the prohibition on slavery, servitude, forced or compulsory labor (Article 4 of ECHR and 8 of the ICCPR), the right to liberty (Articles 5 of the ECHR and 9 of the ICCPR) and freedom of movement (Articles 2 of the Fourth Protocol to the ECHR and 12 of the ICCPR).[236] It would indeed be interesting to consider that these provisions apply as soon as there is "complete and effective control

233. Woodrow Barfield & Alexander Williams, *Law, Cyborgs, and Technologically Enhanced Brains*, PHILOSOPHIES, March 2017, at 11–12; *cf.* Dinniss & Kleffner, *supra* note 23, at 466 ("[W]here soldiers are equipped with cybernetic implants (brain-machine interfaces) which mediate between an information source and the brain, the right to 'receive and impart information without interference from a public authority' gains a new dimension.").

234. Andorno & Ienca, *supra* note 25.

235. ECHR, *supra* note 19, art. 9(1); ICCPR, *supra* note 18, art. 18(1).

236. ECHR, *supra* note 19, arts. 2, 4, 5, 8; ICCPR, *supra* note 18, arts. 8, 9, 12.

over movements." In contrast, both the ECHR (Articles 2 and 3) and the ICCPR (Articles 6 and 7) prohibit remote killing and pain infliction in a satisfactory manner.[237] One of the more disappointing findings of the research is that current understanding of "jurisdiction" is ill-suited to address situations where someone is subject to brain-hacking abroad. The "personal" model of extraterritorial jurisdiction–which requires "power or effective control"[238] or "the exercise of physical power and control"[239] over someon—fails in grasping situations where remote brain-hacking occurs. This proves to be true when someone's thoughts are read, when someone is controlled, and when someone is inflicted pain or killed. This article can only deplore, as other articles before, that the current level of control required to assert jurisdiction is maladjusted to address new technological developments.[240] In contrast, state positive obligations would adapt well to these new challenges, even though the protection of supply chains will be difficult.

IHL, for its part, does not offer further regulation when the thoughts of civilians and prisoners of war are read. However, IHRL regulates this situation in a satisfactory manner, as freedom of thought cannot be derogated from in time of public emergency. However, the remote control of protected persons may be contrary to the laws of war under certain circumstances. For instance, a violation would occur where these persons are placed in "danger zones" or if they are compelled to carry out certain tasks. In addition, acts of violence which are exclusively directed at protected persons shall be prohibited. It means that, if the objective of the brain hacking consists in hurting or killing them, then IHL is breached. Yet, the laws of war would not automatically be violated if a military objective is targeted but that protected persons are incidentally affected. In fact, "collateral damage" is accepted, as long as it is not excessive in relation to the "concrete and direct military advantage anticipated."[241]

---

237. ECHR, *supra* note 19, arts. 2–3; ICCPR, *supra* note 18, arts. 6–7.

238. U.N. Hum. Rts. Comm., *supra* note 36, at ¶ 10.

239. Al-Skeini v. UK, App. No. 55721/07, Eur. Ct. H.R. ¶ 136 (2011), https://www.refworld.org/pdfid/4e2545502.pdf [https://perma.cc/R4TJ-FLJK].

240. Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORDHAM L. REV. 2137, 2151 (2014); Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age,* 56 HARV. INT'L L.J. 81, 120.

241. *Rule 14. Proprionality in Attack*, INTERNATIONAL COMMITTEE OF THE RED CROSS (last visited Sept. 25, 2022, 5:11 PM), https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule14 [https://perma.cc/G2V4-ZMKP].