Introduction

DATA SOCIETY HUMAN RIGHTS AND NEUROTECHNOLOGY

1. *The Data Society*

We have entered the era of data-economy [1]. We have become data-subjects in data societies, a paradigm shift that has transformed the reality we live in, posing novel challenges to which international law (IL) is called to respond [2].

In acknowledging this transformation, the United Nations (UN) has referred to this new world in various and original ways: the Information Society, the Digital Age, the Age of Digital Interdependence, a World that Counts, a Data Revolution for Sustainable Society and the Data Society [3], which entitles this section.

Emerging concepts such as "associative inequality", a consequence of applying data analytics and algorithmic tools to the governance of areas such

---

[1] *Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data*, in *The Economist*, 6 May 2017.

[2] In fact, interest in this field is exponentially growing. See, for instance, the recent creation of International and EU law Interest Group on New Technologies in the Information Society within the Italian Society of International Law.

[3] International Telecommunications Union, *World Summit on the Information Society*, https://www.itu.int/net/wsis/; Office of the High Commissioner for Human Rights, *OHCHR and privacy in the digital age*, https://www.ohchr.org/en/privacy-in-the-digital-age; High-Level Panel on Digital Cooperation, *The Age of Digital Interdependence: Report of the UN Secretary-General's High-Level Panel on Digital Cooperation*, 2019; Independent Expert Advisory Group on a Data Revolution for Sustainable Development, *A World That Counts: Mobilising the Data Revolution for Sustainable Development*, November 2014; UNESCO, *World Trends in Freedom of Expression and Media Development: Global Report 2017/2018*, UNESCO, 2018, p. 3.

as welfare resource allocation [4], border control and migration or even predictive criminality among children [5] illustrate some of the risks resulting from this paradigm shift. Such a trend may lead to replacing the international law principles of solidarity, equality and universal character with discriminatory and biased data-based tools [6]. The IBorderCtrl project is a troubling example of the aforementioned concern. Funded by the EU Commission, this "smart" system for border control claims to be able to detect deception based on facial recognition technology and the measurement of micro-expressions, termed "biomarkers of deceit [7]". From a private perspective, the recent installation of Amazon-Powered AI Cameras in train stations to detect emotion of UK train passengers [8] is equally concerning.

Within armed conflicts, the use of AI-based facial recognition technology to identify targets raises the question that has been extensively dealt with by the scholar community: the compliance of this technology with international humanitarian law [9].

---

[4] RACHOVITSA, A., JOHANN, N., *The human rights implications of the use of AI in the digital welfare state: Lessons learned from the Dutch SyRI case*, in *Human Rights Law Review*, n. 22, 2022, p. 2.

[5] VAN BRAKEL, R., GOVAERTS, L., *Exploring the impact of algorithmic policing on social justice: Developing a framework for rhizomatic harm in the pre-crime society*, in *Theoretical Criminology*, 2024.

[6] VAN DEN MEERSSCHE, D., *Virtual Borders: International Law and the Elusive Inequalities od Algorithmic Association*, in *EJIL*, vol. 33, n. 1, 2022; BROEDERS D., DIJSTELBLOEM, H., *The Datafication of Mobility and Migration Management*, in VAN DER PLOEG, I., PRIDMORE, J. (eds.), *Digitizing Identities: Doing Identity in a Networked World*, Routledge, New York, 2016, pp. 242-3.

[7] SÁNCHEZ-MONEDERO, J., DENCIK, L., *The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl*, in *Information, Communication & Society*, vol. 25, n. 3, 2022, pp. 413 ss.

[8] BURGESS, M., *Amazon-Powered AI Cameras Used to Detect Emotions of Unwitting UK Train Passengers*, in *Wired*, 17th June 2024; available at: https://www.wired.com/story/amazon-ai-cameras-emotions-uk-train-passengers/.

[9] Business & Human Rights Resource Centre, *OPT/Israel: AI used to identify thousands of alleged Hamas targets and to expand facial recognition program in Gaza*, 9th April 2024; available at: https://www.business-humanrights.org/en/latest-news/optisrael-google-corsight-technologies-used-in-israels-expansive-facial-recognition-program-in-gaza/. The human rights implications of resorting to autonomous weapons was already a major concern for the Special Rapporteur on extrajudicial, summary or arbitrary executions in 2013. UN, Human Rights Council, *Report of the Special Rapporteur on extrajudicial, summary of arbitrary executions, Christof Heyns*, A/HRC/23/47, 9th April 2013; ALEGRE, S., *Human Rights, Robots Wrong*. *Being Human in the Age of AI*, Atlantic Books, London, 2024, p. 220.

In all of the above situations, the advent of neurotechnology amplifies the described concerns by enabling direct access to an individual's brain activity. This access not only allows the inference of highly personal and sensitive information through the interpretation of neural data but also creates the potential to alter an individual's mental processes, raising profound ethical and legal challenges.

Neurotechnologies, generally defined as devices and systems that interact with the central nervous system through electrical, magnetic, optogenetic and other means, have only recently transitioned beyond their primary use in the medical field, where they have achieved remarkable advancements in treating neurological disorders. This shift marks their entry into the consumer market, signaling a transformative change as their application to settings such as the workplace, education, and consumer environments introduces unprecedented challenges for the international community to address.

According to the UN's Human Rights Council Advisory Body, which has authored the first UN report on the impact, opportunities and challenges of neurotechnology with regard to the promotion and protection of human rights, there are six aspects of this technology that qualifies it as unique and socially disruptive: they (a) enable the exposition of cognitive processes; (b) enable the direct alteration of a person's mental processes and thoughts; (c) bypass the individual's conscious control or awareness; (d) enable non-consensual external access to thoughts, emotions and mental states; (e) are nurtured by "neurodata", which are needed for their own functioning, calibration and optimization; and (f) collect, analyse and process large personal datasets of a highly sensitive nature [10].

Broadly speaking, the impact of an insufficient protection of personal data on core societal values such as freedom of information or democracy has become a *trending-topic* among research scholars in the last years [11] and has even led the UN Secretary General to concede that some revision of the cur-

---

[10] UN, Human Rights Council, *Impact, opportunities and challenges of neurotechnology with regard to the promotion and protection of all human rights. Report of the Human Rights Advisory Committee*, UN Doc. A/HRC/57/61, 8th August 2024, para. 5.

[11] See, among others, the work of ZUBOFF, S., *Surveillance capitalism*, PublicAffairs, London, 2019; VELEZ, C., *Privacy is power*, Bantam Press, London, 2020; RENIERIS, E.M., *Beyond Data. Reclaiming Human Rights at the Dawn of the Metaverse*, The MIT Press, London, 2023. Attention to this topic is not exclusive from scholars. The proliferation of civil society organizations that focus on research and raising public awareness on this issue is notable. See, among others: https://www.article19.org; https://www.luminategroup.com.

rent systems of protection might be needed as "the existing human rights treaties were signed in a pre-digital era [12]".

While some researchers have focused on examining the risks of corporate collection and exploitation of this data [13], others have concentrated on shedding the light on human rights violations committed both by democratic and authoritarian States through surveillance [14], biometric data-based repression of political opposition or through the adoption of social of reputation scoring systems [15]. Concerns on how the inadequate regulation of facial recognition technologies may impact the rights of future generations have also been raised by the Special Rapporteur on the right to development [16]. If neural data were to become accessible, there is little reason to doubt that this particularly sensitive category of data could similarly be exploited for such purposes.

There are two events which are generally referred to as the turning point in the context of personal data misuse for manipulative and spyware purposes. These cases proved experts right by confirming, in practice, many of the fears and risks against which the international community had been warning for years: the Cambridge Analytica scandal and the Pegasus Project case.

The Cambridge Analytica scandal [17] saw about 87 million Facebook users have their data analysed for political purposes [18] evidencing, for the first time in a wide scale, the impact that behavioral microtargeting, based on algorithms created from our data, may have on core societal values such as democracy. Conversely, the Pegasus Project [19] led to the release of a report

---

[12] UN Secretary-General, *'Road Map for Digital Cooperation: Implementation of the Recommendations of the High-Level Panel on Digital Cooperation'*, 29th May 2020, UN Doc A/74/821, para. 38.

[13] MALGIERI, G., *In/acceptable marketing and consumers' privacy expectations: four tests from EU data protection law*, in *Journal of Consumer Marketing*, vol. 40, n. 2, 2023, pp. 209-23.

[14] ZALNIERIUTE M., *Big Brother Watch and Others v. the United Kingdom*, in *American Journal of International Law*, vol. 116, n. 3, 2022, pp. 585-92.

[15] DI CARPEGNA BRIVIO, E., *Pari dignità sociale e Reputation scoring. Per una lettura costituzionale della società digitale*, Giappichelli, Torino, 2024.

[16] GA, HRC, *Right to development of children and future generations. Report of the Special Rapporteur on the right to development, Surya Deva,* Doc. n. A/HRC/57/43, 24th July 2024, p. 17, para. 80.

[17] Https://www.theverge.com/2018/4/10/17165130/facebook-cambridge-analytica-scandal.

[18] BBC, *Facebook fined $500,000 for Cambridge Analytica scandal*, 25th October 2018; available at: https://www.bbc.com/news/technology-45976300.

[19] It is not difficult to identify worldwide examples technology-based political repression

by an investigative consortium of 17 organizations, including Amnesty International. The report alleged extensive misuse of NSO's spyware, Pegasus, which had been employed by governments worldwide to hack activists, journalists, and politicians since 2016. The analysis conducted by the consortium identified at least 11 governments believed to be NSO customers who were entering numbers into a system: Azerbaijan, Bahrain, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, Togo, and the United Arab Emirates [20].

Against this backdrop, and despite the examined precedents that could have been expected to heighten awareness about personal data protection, cultural differences in public trust toward state use of personal data for security and law enforcement purposes add another layer of complexity to the challenge of establishing an international framework for the protection of biometric data (and, eventually, neural data). For instance, a 2015 survey by the European Union Fundamental Rights Agency (FRA), which included 1,227 third-country nationals, found that 12% of respondents felt very uncomfortable with the use of their facial image for border crossing, 18% considered it a significant intrusion into their privacy, and 26% described the practice as humiliating [21]. In contrast, a 2019 report by the Pew Research Center revealed that 56% of Americans trusted law enforcement agencies to use such technologies responsibly [22].

---

beyond the Pegasus case. Under Hong Kong's recent national security law (also known as art. 23) treason, insurrection and sabotage can be punished with life sentences, while jail terms for sedition are increased from two years to seven, or 10 if alleged perpetrators are found to have colluded with a foreign force. The law, which arrives only 5 years after the pro-democracy protests was passed by pro-Beijing legislators to suppress public demonstrations against the government. This reform raises human rights concerns in a country which is known to resort to facial recognition and the collection of biometric data for repressive purposes. MOZUR, P., *In Hong Kong Protests, Faces Become Weapons*, in *The New York Times*, 26th July 2019; available at: https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.

[20] Business and Human Rights Resource Centre, *Investigation finds NSO Group spyware sold to governments used against activists, politicians & journalists; company denies allegations*, 27th September 2021; available at: https://www.business-humanrights.org/en/latest-news/nso-group-spyware-sold-to-governments-used-to-target-activists-politicians-journalists-according-to-pegasus-project-investigation-company-denies-allegations/.

[21] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2020, pp. 8 ss.

[22] SMITH, A., *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, 5th September 2019; available at: https://www.pewresearch.org/int

2. *"Voluntary" disclosure of personal and neural data*

Personal data is however not always stolen, hacked or collected in an abusive way. From a regulatory standpoint, this aspect poses in fact some of the more complex challenges. In her book "The Quantified Self", University of New South Wales (Sydney) professor Deborah Lupton carries out a critical examination of contemporary self-tracking practices defined as practices directed at regularly monitoring and recording, and often measuring, elements of an individuals' behaviour or bodily functions knowingly and purposively by the individual [23]. In recent times, this includes brain-function monitoring devices that provide the user information about concentration levels or emotional states [24]. While the medical nature of neural data and its classification as highly sensitive data remain subjects of debate, there is there is broad consensus that neural data falls within the category of personal data [25].

The voluntaristic or consented disclosure of personal data has even led some authors to hold that while initially the data market was controlled by a few companies that collected and used data for their own benefit, the new data-business models that start to emerge, such as the "pay-for-privacy" or the "personal data economy" would suggest a shift in this trend which may result from increasing awareness of privacy risks and/or consumer empowerment [26].

In the context of data-sharing, recent studies have shown that not only cultural but generational factors may condition consumers' willingness to share their personal data in exchange for services [27]. However, in a recently

---

ernet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/.

[23] LUPTON, D., *The Quantified Self*, Cambridge University Press, Cambridge, 2016, pp. 2-3.

[24] PEAKE, J.M., KERR, G., SULLIVAN, J.P., *A Critical Review of Consumer Wearables, Mobile Applications, and Equipment for Providing Biofeedback, Monitoring Stress, and Sleep in Physically Active Populations*, in *Front. Physiol*., vol. 28, 9th June 2018, p. 743.

[25] See section 2 of chapter 3: Neural data and the right to privacy.

[26] ELVY, S.A., *Paying for Privacy and the Personal Data Economy*, in *Columbia Law Review*, vol. 117, n. 6, 2017.

[27] MILTGEN, C., PEYRAT-GUILLARD, D., *Cultural and generational influences on privacy concerns: A qualitative study in seven European countries.*, in *European Journal of Information Systems*, vol. 23 (2), 2014, p. 29. For a comparison between the Indian and American consumer, see GUPTA, B., IYER, L., WEISSKIRCH, R., *Facilitating global e-commerce: A comparison of consumers' willingness to disclose personal information online in the U.S. and in India*, in *Journal of Electronic Commerce Research*, 11, 2010.

non-binding Opinion, the European Data Protection Board (EDPB) has expressed the view that large platforms such as Facebook and Instagram cannot force a "binary" pay or consent choice on users [28]. In order to ensure that all the relevant elements [29] are taken into consideration when assessing the informed, specific and unequivocal nature of the consent provided by the users, the EDPB is committed to developing guidelines on the "consent or payment" models with a wider scope.

This been said, increasing awareness at an institutional level and isolated virtuous market trends should not divert our attention from a more comprehensive analysis of the problem at stake, which suggests that the unregulated proliferation of social media platforms that commodify information by trading in influence through personal data [30], has consolidated a new industry that poses unprecedented risks to human rights.

These risks are amplified when combined with artificial intelligence (AI), specifically from the inferences perspective [31]. As it has historically occurred with other industries such as cars, tobacco and chemicals, the data technology sector has enjoyed a period of relative lawlessness and exceptional treatment [32] which seems to be coming to an end [33].

---

[28] European Data Protection Board, *EDPB: Consensus or Payment Models should offer a real choice*, 17th April 2024; available at: https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_it#:~:text=As%20regards%20'consent%20or%20pay,personal%20data%20for%20behavioural%20advertising. This opinion was released almost a year after the ECJ's decision in the Meta Platforms Inc. Bundeskartellmant case (C-252/21) from the 4th July 2023 addressed the intersection between data protection and competition law, ruling that Meta's data processing practices, which involve collecting user data across its services and other third-party websites, required explicit user consent under the GDPR. This was found to be so even in cases where services are provided free of charge. ECJ, Meta Platforms Inc and Others v Bundeskartellamt, case C-252/21, Judgement of the Court (Grand Chamber) of 4th July 2023. ECLI identifier: ECLI:EU:C:2023:537. For a comment on this decision see VAN DE WAERDT, P., *Meta v. Budeskartellamt: something old, something new*, in *European Papers*, vol. 8, n. 3, pp. 1077-1103.

[29] This includes the existence of an imbalance of power between the individual and the data-controller, the extent to which the individual relies on the service and the primary public of the service.

[30] VELEZ, C., *Privacy is power*, Bantam Press, London, 2020, p. 18.

[31] KELLMEYER, P., *Big Brain Data: On the Responsible Use of Brain Data from Clinical and Consumer-Directed Neurotechnological Devices*, in *Neuroethics*, 14, 2021, pp. 83-98.

[32] RENIERIS, E.M., *Beyond Data. Reclaiming Human Rights at the Dawn of the Metaverse*, The MIT Press, London, 2023, pp. 124-5.

[33] At the European level, the EU Commission's strategy for Europe in the digital age, "A Europe fit for the digital age", enshrines a series of regulatory initiatives that consolidate the

Against this background, this book's main goal is to look at these and other problems with respect to neurotechnology, an emerging technology based on the collection, interpretation and potential alteration of a particular type of data, a data that interacts with the essence of the self[34]: neural data.

Before delving into the topic, it should be clarified that this book will follow the Ad Hoc Expert Group recently appointed by UNESCO to prepare a Recommendation on the ethics of neurotechnology, which has opted for the term "neural data" over other terms that had been coined by the doctrine such as mental data or brain data[35]. In this draft report, neural data is defined as "quantitative data about the structure, activity and function of the nervous system of a living[36]".

EU's role as a leader of a rights-driven and human-centred regulatory model for digital technologies. BRADFORD, A., *Digital Empires. The Global battle to regulate technology*, Oxford University Press, New York, 2023, p. 105; MANTELERO, A., *Regulating AI*, in *Beyond Data. Information Technology and Law Series*, vol. 36, T.M.C. Asser Press, The Hague, 2022, pp. 139-83; ALMADA, M., RADU, A., *The Brussels Side-Effect: how the AI Act can reduce the global reach of EU Policy*, in *The German Law Review*, 25, 2024, pp. 646-63.

[34] According to the founder of the Neurorights Foundation, Rafael Yuste, neurotechnologies have the potential of changing the concept of what it is to be human. If this is not a human rights problem, what is?

[35] Brain data is used as a synonym of neural data both in the literature and in some important policy documents. GOERING, S., KLEIN, E., SPECKER SULLIVAN, L. *et al*., *Recommendations for Responsible Development and Application of Neurotechnologies*, in *Neuroethics*, vol. 14, 2021, p. 371; IENCA, M., *Common human rights challenges raised by different application of neurotechnologies in the biomedical field*, Report commissioned by the Committee on bioethics (DH-BIO), 2021.

[36] UNESCO, *Outcome document of the first meeting of the AHEG. First Draft of a Recommendation on the ethics of neurotechnology (first version)*, Doc. n. SHS/BIO/AHEG-Neuro/2024/1.REV, p. 5, para. 7-8. The group held its first meeting from the 22-26 April 2024 and its first draft text was opened to global regional and national consultations between May and July 2024. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000389768. Following the consultations, in October 2024, UNESCO published the First Draft of the Recommendation on the Ethics of Neurotechnology, which is expected to be discussed with Member States in Spring 2025. This draft defines neural data as "qualitative and quantitative data about the structure, activity and function of the nervous system". UNESCO, *First Draft of the Recommendation on the Ethics of Neurotechnology*, Doc. n. SHS/BIO/AHEG-Neuro/2024/2, p. 4, para. 15. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000391444.locale=es.

3. *Structure of the book*

The book is structured as follows. In line with the interdisciplinary efforts made by a part of the international law scholarship [37], Part I will concentrate on framing the research question by proposing a dialogue between science and law. To this end, following an in-depth analysis of the theoretical foundations on which the international soft law regulation of emerging technologies is grounded, chapter 2 will be dedicated to defining neurotechnology (NT), its applications and the potential impacts on human rights that derive from it, hopefully shedding some light on the reasons that have led the international community to stress the urgency of adopting a global governance framework in this context.

Part II will examine the different areas of IL that may be affected by the proliferation of neurotechnologies. In this regard, while chapter 3 will focus on the international human rights framework with special attention to the so-called negative rights, chapter 4 will explore the potential impact of neurotechnologies on the Agenda 2030 and on the Sustainable Development Goals (SDGs). Ultimately, chapter 5 will look into the dual-use nature of the product under consideration, with specific attention to the military uses of neurotechnology and their compliance with International Humanitarian Law (IHL).

Part III of the book will delve into the multi-level regulatory and governance response to the emergence of neurotechnology. In this realm, chapter 6 will specifically focus on the soft law proposals that have been adopted by international and regional organisations such as UNESCO, the OECD, the UN Human Rights Council, the Council of Europe, the European Union and the Organization of American States (OEA). Finally, chapter 7 will concentrate on the current and future governance of neurotechnologies. In this last chapter, which combines descriptive and prescriptive elements, attention will be paid to the challenges encountered by the competent authorities when enforcing such a *sui generis* normative system.

For the reasons explained above, the topic under consideration requires resorting to a combination of IL methodologies [38]. On one side, given the

[37] The theme of the American Society of International Law last call for papers for the Conference that will take place at the Northwestern Pritzer School of Law on the 27-28 September 2024 was specifically on the topic: "Building New Interdisciplinary Networks".

[38] Such an approach is in line with recent trends in international law scholarship. See, for instance, Arcari's assessment on the importance of dealing with the challenges posed by emerging technologies at the three levels of space, actors and governance in an insightful

human rights implications resulting from the use of neurotechnologies, a comprehensive assessment of the existing international human rights system of protection's capacity to address the unprecedented threats posed by the advancement of this technology will be carried out. On the other side, the role that soft law is called to play in the context of neurotechnology international governance requires attention from a publicist perspective for three reasons: the rising trend to resort to soft law instruments to regulate highly technical global challenges (in particular in the scope of digital technologies requiring anticipatory governance frameworks); the triple function of soft law instruments and their capacity to inspire, interpret or substitute international law and the illusion of enforceable international law in the contemporary geopolitical scenario [39].

Ultimately, this monographic work aims to answer a research question that may be broken down into two parts:

1. Does the international human rights system of protection provide the adequate regulatory framework in the light of the unprecedented challenges posed by NT?
2. What role can be acknowledged to soft law instruments in enabling the reformulation or updated interpretation of preexistent human rights in this context?

This book will contend that by modernizing or reconceptualizing existing human rights using mechanisms available within the international human rights system, such as the General Comments of Treaty Bodies, it is possible to provide protection against the emerging threats posed by the proliferation of neurotechnologies. It will also be argued that, in light of recent advancements in international law, a new soft law framework developed collaboratively at the international level by the UN and UNESCO could be essential for globally strengthening human rights protections in the context of neurotechnology.

---

collective work on the challenged that the use and misuse of emerging technologies pose for International and European Law. ARCARI, M., *New Technologies in International (and European) Law – Contemporary Challenges and Returning Issues*, in CARPANELLI, E., LAZZERINI, N. (eds.), *Use and Misuse of New Technologies*, Springer, Cham, 2019.

[39] Where multilateralism seems to be giving place to regionalization and where cooperation in terms of ensuring standards to protect human rights in Data Societies seem to occur within bilateral/regional contexts. See, for instance, the US-EU Technology trade council, the EU Commission's decision to engage in digital diplomacy recognizing 13 countries as providing adequate level of protection for personal data. European Commission, *A European strategy for data*, COM (2020) 66 final, 19th February 2020, p. 4.