

# The insufficiency of technology neutrality and risk-based approaches: The necessity of adopting a human-rights lens when regulating AI

*Machi Tsokou*

## I. Introduction

Depending on the lens we choose to look at it, AI covers many disciplines and functions. It is a set of technologies, but it can also be defined as a field of science and philosophy. The versatile character of AI as a discipline is also illustrated by the functions it covers. In the beginning of its lifetime, Deep Blue was able to defeat Kasparov in chess. Nowadays, AI systems can affect the market<sup>1</sup>, impact healthcare<sup>2</sup> and contribute to the creation of smart cities<sup>3</sup>. This drastic change corresponds to an increased need for regulation.

The European regulatory agenda has only recently addressed AI. The European Commission developed a strategy to accord to the European approach to AI, which is focused on research and policy measures for its regulation<sup>4</sup>. In addition, the Commission published a package including new rules to achieve two goals: trust and excellence in AI<sup>5</sup>. Included in these efforts is the proposed Artificial Intelligence Act aiming to harmonize rules on AI across Member States<sup>6</sup>.

Throughout the regulatory process, various principles and approaches can be used to achieve desired goals. The principle of technology neutrality dictates that the same regulatory principles should apply regardless of the technology used<sup>7</sup>. The human rights approach, instead of a risk-based approach which is followed in Commission's 2020 White paper on Artificial Intelligence<sup>8</sup>, advocates for consideration of fundamental rights. The goal of this essay is to advocate for a human rights lens to complement the technology neutral approach adopted by European regulators thus far. To illustrate this opinion, the Artificial Intelligence Act is used as an example of a measure that could be further harmonized with human rights.

---

<sup>1</sup> Alessio Azzutti, Wolf-Georg Ringe & H. Siegfried Stiehl, *Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" matters*, SSRN JOURNAL (2021), <https://www.ssrn.com/abstract=3788872> (last visited Sep 16, 2021).

<sup>2</sup> 37 AI In Healthcare Examples You Should Know | Built In, <<https://builtin.com/artificial-intelligence/artificial-intelligence-healthcare>> (last visited Sep 16, 2021).

<sup>3</sup> European Parliament Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies (IPOL), *Artificial Intelligence in smart cities and urban mobility* (last visited Sep 23, 2021).

<sup>4</sup> European Commission, *A European Approach to artificial intelligence*, <<https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>> (last visited Sep 23, 2021).

<sup>5</sup> *ibid.*

<sup>6</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM/2021/206 final.

<sup>7</sup> Winston James Maxwell and Marc Bourreau, 'Technology Neutrality in Internet, Telecoms and Data Protection Regulation' [2014] SSRN Electronic Journal <<http://www.ssrn.com/abstract=2529680>> accessed 24 September 2021.

<sup>8</sup> European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust* COM (2020) 65 final.

Against this backdrop, this essay sets out by explaining technology neutrality and its successful application in the General Data Protection Regulation (GDPR)<sup>9</sup>. Then, the essay proposes human rights as a suitable lens to regulation (Section III). Finally, this essay suggests improvements of the Artificial Intelligence Act hinting towards how the human-rights lens can be substantiated (Section IV). Section V concludes.

## II. The use of Technology Neutrality in AI Regulation

The principle of technology neutrality is fundamental for proper regulation of technology due to the liberalization of the telecommunications market<sup>10</sup>. In Europe, technology neutrality had its debut in electronic communications regulation<sup>11</sup>. Its existence commences in 2002, while it was first reinforced in 2009 with revised EU telecoms legislation<sup>12</sup>. Technology neutrality serves various legislative purposes. Koops argues that it brings forth achievement of specific effects in terms of behavior or activities; the functional equivalence between different modes of activity; the non-discrimination between technologies with equivalent effects; and the futureproofing of law<sup>13</sup>. Futureproofing according to Koops is the drafting of laws in a way flexible enough not to hinder future development of technology, and the achievement of sustainability in the sense of abolishing the need of constant legal revision<sup>14</sup>. When discussing this principle, this essay refers to its futureproofing purpose.

Creating legislation that can survive the current of constant technological advancements is challenging. Regulating too closely to technology can hinder technical progress<sup>15</sup>. Futureproofing insinuates that the same regulatory principles and rules apply regardless of the technology. The very nature of AI calls for the application of technology neutrality. Though AI technology can be thought of as a self-descriptive term, the reality is that various technologies fall under its umbrella. AI technology includes and is not limited to machine learning, expert systems, planning, machine vision, natural language processing and robotics. Therefore, technology neutrality is essential in encompassing the vast number of systems and technologies classified as ‘AI’ in regulation.

---

<sup>9</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2016 L 119/1 (hereinafter ‘GDPR’).

<sup>10</sup> Chris Reed, ‘Taking Sides on Technology Neutrality’ (2007) 4 SCRIPT-ed 263 <<http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp>> (last visited Sep 23, 2021).

<sup>11</sup> Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). See also Technology neutrality in Internet, telecoms and data protection regulation, GLOBAL MEDIA AND COMMUNICATIONS WATCH (2014), <https://www.hlmediacomms.com/2014/11/17/technology-neutrality-in-internet-telecoms-and-data-protection-regulation/> (last visited Sep 16, 2021).

<sup>12</sup> *ibid*

<sup>13</sup> Bert-Jaap Koops, "Should ICT Regulation be Technology-Neutral" in Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, Starting Points for ICT Regulation: deconstructing prevalent policy one-liners (The Hague: TMC Asser Press 2006).

<sup>14</sup> See Chris Reed, ‘Taking Sides on Technology Neutrality’ (2007) 4 SCRIPT-ed 263 <<http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp>> (last visited Sep 23, 2021).

<sup>15</sup> Juan Murillo Arias, ‘What Should Be Taken into Account If Artificial Intelligence Is to Be Regulated?’ (*Finextra Research*, 26 October 2020) <<https://www.finextra.com/the-long-read/62/what-should-be-taken-into-account-if-artificial-intelligence-is-to-be-regulated>> accessed 21 September 2021.

Legal futureproofing is inextricably linked with the notion of legal disruption. Disruptive AI implies a situation where the technology has a truly disruptive impact on the already existing regulatory model, hence requiring a new updated model. With technology neutrality this burden is avoided. By creating a framework that is neutral, all AI will likely fall under this framework in any instance and requires a breakthrough event (an affordance) to substantially challenge it.

Aside from providing a longer lifespan to legislation, this principle provides flexibility to regulators. Specifically, it pressures regulated entities to find self-regulatory solutions<sup>16</sup>. This is a special characteristic of technology neutrality vis-à-vis a technology-focused approach. Not only flexibility is enhanced, but technology neutrality also allows for consideration of social and economic factors. For instance, pushing the market into self-regulatory or co-regulatory solutions that can be more effective than strict regulation.

‘Privacy by design’ in the GDPR is an example of co-regulation<sup>17</sup>. It allows a discretion for entities in selecting appropriate technical and organizational measures<sup>18</sup>. In fact, the GDPR is the most significant measure in the European Union (EU) that can be characterized as technology neutral. This is because it protects personal data regardless of the technology used for a processing operation or its storage. There is no difference in the eyes of the GDPR if data is filed in a modern IT system or on papyrus paper. In particular, the GDPR cites that ‘In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used’<sup>19</sup>.

To regulate in a technology specific manner requires to clearly outline the purposes and scope of the regulation,<sup>20</sup> but AI has a broad and even unexplored scope. Consequently, technology neutrality is valuable in enshrining a definition of AI systems<sup>21</sup>. The broad proposed definition by the Commission Communication on AI abides by this principle. Namely, ‘Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals’<sup>22</sup>.

Though already applied in EU legislation, technology neutrality cannot be the only tool in the toolbox when regulating AI. Indeed, the GDPR constitutes a successful example of its implementation because it provides control to data subjects, individuals, consumers over their

---

<sup>16</sup> Guy Halfteck, ‘Legislative Threats’ (2008) 61 Stanford Law Review.

<sup>17</sup> GDPR art 25 and recital 78.

<sup>18</sup> *ibid.*

<sup>19</sup> GDPR recital 15.

<sup>20</sup> Juan Murillo Arias, ‘What Should Be Taken into Account If Artificial Intelligence Is to Be Regulated?’ (*Finextra Research*, 26 October 2020) <<https://www.finextra.com/the-long-read/62/what-should-be-taken-into-account-if-artificial-intelligence-is-to-be-regulated>> accessed 21 September 2021.

<sup>21</sup> European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Fostering a European approach to Artificial Intelligence COM (2021) 205 final.

<sup>22</sup> European Commission’s High-Level Expert Group on Artificial Intelligence (AI HLEG), ‘A Definition of AI: Main Capabilities and Scientific Disciplines’ (2018).

data. However, AI regulation should be approached from an additional perspective. To advocate only for technology neutrality to underlie these efforts would be superficial. As shown by the extreme yet humorous Mulching Proposal, when a prominent regulatory framework is applied to an algorithm which renders down the elderly into a fine nutrient slurry, ‘the problem is not how the sausage gets made, but that they’re making people into sausage’<sup>23</sup>. Consequently, this essay further argues that adopting a holistic human rights perspective, instead of technology neutrality or a risk-based approach, can tackle deeper issues. As stated by OHCHR Director of Thematic Engagement: ‘It is not about the risks in future, but the reality today. Without far-reaching shifts, the harms will multiply with scale and speed, and we won't know the extent of the problem’<sup>24</sup>.

### III. The human rights approach

Insisting on the adoption of a human rights lens presupposes that several philosophical debates have been settled<sup>25</sup>. At the European level, this assumption is diminished due to a common human rights culture. Besides the Universal Declaration of Human Rights<sup>26</sup>, European Union (EU) Member States abide by legal instruments including the European Convention of Human Rights<sup>27</sup> as well as the Charter of Fundamental Rights of the EU<sup>28</sup>.

A challenge exists in creating techno-regulation that abides by a deeper level of legitimacy<sup>29</sup>. This challenge is rooted in the perfect enforcement of techno-regulation that potentially deprives the moral freedom rooted on the fact that ‘humans should do the right things’<sup>30</sup>. However, the only way to deal with such dilemmas is to find anchor points. In the EU, the common heritage of fundamental rights serves as such an anchor point. Though theoretically simple, the presence of human rights and values requires continuous attention to address unexpected side effects and could affect other rights or values, as well as to address any significant updates<sup>31</sup>. Thus, the adoption of a human rights lens is connected to the great risk of constitutional rights becoming vague, thereby diluting constitutional protection, that is posed by technology neutrality.

---

<sup>23</sup> Os Keyes, Jevan Hutson and Meredith Durbin, ‘A Mulching Proposal’ [2019] arXiv:1908.06166 [cs] <<http://arxiv.org/abs/1908.06166>> accessed 23 September 2021.

<sup>24</sup> United Nations, ‘Urgent Action Needed over Artificial Intelligence Risks to Human Rights’ (*UN News*, 15 September 2021) <<https://news.un.org/en/story/2021/09/1099972>> accessed 23 September 2021.

<sup>25</sup> Mathias Risse, ‘Human Rights and Artificial Intelligence: An Urgently Needed Agenda’ (2019) 41 *Human Rights Quarterly* 1 <<https://muse.jhu.edu/article/716358>> accessed 21 September 2021.

<sup>26</sup> UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), art 12.

<sup>27</sup> Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, as amended by Protocols Nos. 11 and 14 [1950] ETS 5, arts 7 and 8.

<sup>28</sup> Charter of Fundamental Rights of the European Union [2012] OJ C326/391 (hereinafter ‘the Charter’), art 8.

<sup>29</sup> Ronald Leenes and others, ‘Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues’ (2017) 9 *Law, Innovation and Technology* 1 <<https://doi.org/10.1080/17579961.2017.1304921>> accessed 23 September 2021.

<sup>30</sup> *ibid.*

<sup>31</sup> Ronald Leenes and others, ‘Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues’ (2017) 9 *Law, Innovation and Technology* 1 <<https://doi.org/10.1080/17579961.2017.1304921>> accessed 23 September 2021.

Even in the EU, only recently has technology regulation considered human rights such as privacy and data protection. Indeed, it can be held that a tendency exists to only think of privacy and data protection when dealing with technology regulation. Notwithstanding, a holistic human rights approach is needed to address AI because it threatens more than a few fundamental rights. The creation of a legal framework for the development, design and application of AI needs to be based on human rights standards, democracy, and the rule of law<sup>32</sup>. Hildebrandt and Tielemans point out that technology neutral law might also require some technology specifics to prevent technological threats to human rights<sup>33</sup>. Barbora Bukovska stresses that ‘if the EU wants to be a leader in AI regulation, it must go much further in protecting rights. As it stands, many types of extremely invasive biometric mass surveillance and other unacceptable uses of AI systems could be allowed in the future, with a significant impact on human rights’<sup>34</sup>. The unprecedented level of mass surveillance following the Pegasus spyware controversy has been characterized by UN Rights Chief as ‘incompatible’ with human rights<sup>35</sup>.

The question arises how fundamental rights are impacted from this. AI triggers numerous fundamental rights but this essay focuses on four of them, namely the right to equality, the prohibition of discrimination, and the rights to privacy and data protection.

The violation of the latter two rights is based on the ability of AI systems to make personal predictions on processed and stored data, to create a full idea of individuals’ lives, even its more private aspects. These aspects include data that can be classified as sensitive under the GDPR regime, including biometric data. An example of a risk compromising biometric data is the use of AI systems in public spaces for real-time facial-recognition purposes, or even unlimited tracking<sup>36</sup>. Therefore, it is both an issue of the data itself being compromised and then its further use. Due to the black-box nature of algorithms, meaning their opaque nature and inability of outside oversight, such sensitive data can be stored for an unlimited timeframe or even be unlawfully used for other purposes.

The term sensitive data under the GDPR includes data on individuals’ political, philosophical, religious views, as well as sexual orientation. This aspect is linked with the violation of non-discrimination and the right to equality. This is because AI can make bigger decisions such as political views, suitability for a job, scan crowds, sentencing and parole decisions or access to social welfare<sup>37</sup>. Again, the black-box nature of algorithms can lead to bias and an unclear impact on these rights. The first issue per se is the predictive ability of AI systems, which can

---

<sup>32</sup> Marija Pejčinović Burić, ‘Artificial Intelligence and Human Rights’ (*Council of Europe Portal*) <<https://www.coe.int/en/web/artificial-intelligence/secretary-general-marija-pejcinovic-buric>> accessed 23 September 2021.

<sup>33</sup> Mireille Hildebrandt and Laura Tielemans, ‘Data Protection by Design and Technology Neutral Law’ (2013) 29 *Computer Law & Security Review* 509 <<https://www.sciencedirect.com/science/article/pii/S0267364913001313>> accessed 23 September 2021.

<sup>34</sup> ‘EU: New Proposal on Artificial Intelligence Must Protect Human Rights’ (*ARTICLE 19*, 2021) <<https://www.article19.org/resources/eu-artificial-intelligence-and-human-rights/>> accessed 23 September 2021.

<sup>35</sup> United Nations, ‘Urgent Action Needed over Artificial Intelligence Risks to Human Rights’ (*UN News*, 15 September 2021) <<https://news.un.org/en/story/2021/09/1099972>> accessed 23 September 2021.

<sup>36</sup> *ibid.*

<sup>37</sup> *ibid.*

detect behavior and according to it take discriminatory decisions. Linked to this is the risk associated with the principle of transparency. Transparency is lacking in the decision-making process of algorithms, accountability mechanisms, the designation of safeguards if any, and lastly how algorithms can evolve over time<sup>38</sup>. Therefore, the process and consequences of an AI system's decision are unclear to individuals. The absence of effective redress mechanisms able to meaningfully explain these decisions and demand human involvement in their oversight darkens the grey cloud that covers AI.

Transparency is not the only concept that challenges the prohibition of non-discrimination and the right to equality. Bias constitutes a basic ingredient in discriminatory and unequal decisions taken by AI systems. Because machines operate on data inserted by humans, which can oftentimes be amongst others socially and politically biased, the result will inevitably be biased. These results can further discrimination and reinforce biases and prejudices of society<sup>39</sup>. In 2015, racial discrimination was fortified by Google Photos, an advanced recognition software, which categorized two images of black people as pictures of gorillas<sup>40</sup>. Social discrimination underpinned Google's ad policy, where women were less likely to be shown ads for high-paid jobs contrary to men<sup>41</sup>. In both cases, the AI systems concerned failed to ensure a standard of equality leading to discriminatory results<sup>42</sup>. The gravity of the infringing results can vary from a Google search appearance to the conviction of individuals due to biased AI criminal justice systems able to enhance pre-existing discriminatory law enforcement practices<sup>43</sup>.

Risks towards human rights are various, some of them yet conceived. The use of any other basis to regulation besides human rights would imply a short-sighted attitude. Regulation should be technology neutral, so that the higher the risk for human rights, the stricter the legal requirements are<sup>44</sup>. Due to the obscurity of future results, decisions and abilities of AI

---

<sup>38</sup> Dunja Mijatović, 'Safeguarding Human Rights in the Era of Artificial Intelligence' (*Council of Europe Portal*, 2018) <[https://www.coe.int/en/web/commissioner/blog/-/asset\\_publisher/xZ32OPEoxOkq/content/safeguarding-human-rights-in-the-era-of-artificial-intelligence](https://www.coe.int/en/web/commissioner/blog/-/asset_publisher/xZ32OPEoxOkq/content/safeguarding-human-rights-in-the-era-of-artificial-intelligence)> accessed 23 September 2021.

<sup>39</sup> European Union Agency for Fundamental Rights, '#BigData: Discrimination in data-supported decision making' (2018).

<sup>40</sup> Natasha Singer and Cade Metz, 'Many Facial-Recognition Systems Are Biased, Says U.S. Study' *The New York Times* (19 December 2019) <<https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html>> accessed 23 September 2021. See also Sahajveer Baweja and Swapnil Singh, 'Beginning of Artificial Intelligence, End of Human Rights' (*LSE*) <<https://blogs.lse.ac.uk/humanrights/2020/07/16/beginning-of-artificial-intelligence-end-of-human-rights/>> accessed 23 September 2021.

<sup>41</sup> Samuel Gibbs, 'Women Less Likely to Be Shown Ads for High-Paid Jobs on Google, Study Shows' *The Guardian* (8 July 2015) <<https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study>> accessed 23 September 2021.

<sup>42</sup> Natasha Singer and Cade Metz, 'Many Facial-Recognition Systems Are Biased, Says U.S. Study' *The New York Times* (19 December 2019) <<https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html>> accessed 23 September 2021. See also Sahajveer Baweja and Swapnil Singh, 'Beginning of Artificial Intelligence, End of Human Rights' (*LSE*) <<https://blogs.lse.ac.uk/humanrights/2020/07/16/beginning-of-artificial-intelligence-end-of-human-rights/>> accessed 23 September 2021.

<sup>43</sup> Odhran James McCarthy, 'AI & Global Governance: Turning the Tide on Crime with Predictive Policing' *United Nations University Centre for Policy Research* (2019) <<https://cpr.unu.edu/publications/articles/ai-global-governance-turning-the-tide-on-crime-with-predictive-policing.html>> accessed 23 September 2021.

<sup>44</sup> United Nations, 'Urgent Action Needed over Artificial Intelligence Risks to Human Rights' (*UN News*, 15 September 2021) <<https://news.un.org/en/story/2021/09/1099972>> accessed 23 September 2021.

systems, human rights should accompany, and even overpower, technology neutrality or risk-based approaches.

The above-mentioned risks correspond to certain recommendations to mark the way forward. On a broader spectrum, closer co-operation between state actors, private companies, NGOs, academia, and civilians would create a better environment for regulation and oversight<sup>45</sup>. More specifically, clear redress and oversight mechanisms can deal with AI systems' results. However, human oversight is not sufficient if it only deals with problems after they occur. As a result, there is a need for techniques able to predict outcomes and meaningfully explain AI<sup>46</sup>. Employing a framework of oversight and prediction implies that algorithms need to be assessed in terms of their lawfulness, the quality of data used and the underlying transparency via audits or impact assessments<sup>47</sup>. Like the GDPR, the possibility to review decisions with a human actor and have them be meaningfully explained could be valuable<sup>48</sup>. Lastly, for the most effective implementation of regulation, already existing standards should be used or even enhanced. Human rights standards enshrined in treaties and legislation should be reinforced. To this end, the next section approaches the proposed Artificial Intelligence Act as an instrument that could be improved to enhance fundamental rights protection.

#### **IV. The Artificial Intelligence Act**

Commission's 2020 White paper on Artificial Intelligence aimed for the application of a risk-based approach to the Artificial Intelligence Act<sup>49</sup>. This approach involves the determination of the scale or scope of risks related to a concrete situation and a recognizable threat. The proposed rules (i) address specific risks created by AI systems, (ii) propose a list of high-risk systems, (iii) set clear requirements for high-risk systems, (iv) define specific obligations for AI users and providers, (v) propose the conduction of a conformity assessment before such system enters the market, (vi) propose enforcement after its placement and lastly (vii) propose a governance structure at the national and European levels<sup>50</sup>. The categorization of systems into unacceptable risk, high-risk, limited risk and minimal risk is promising at first. In practice, tech giants would need to evaluate their operational risks vis-à-vis individuals' fundamental rights. However, fundamental rights although not absolute cannot be balanced out by companies' interests. This is because when applied in practice, the Act will allow companies to under evaluate human rights in the name of new product launches.

---

<sup>45</sup> Dunja Mijatović, 'Safeguarding Human Rights in the Era of Artificial Intelligence' (*Council of Europe Portal*, 2018) <[https://www.coe.int/en/web/commissioner/blog/-/asset\\_publisher/xZ32OPEoxOkq/content/safeguarding-human-rights-in-the-era-of-artificial-intelligence](https://www.coe.int/en/web/commissioner/blog/-/asset_publisher/xZ32OPEoxOkq/content/safeguarding-human-rights-in-the-era-of-artificial-intelligence)> accessed 23 September 2021.

<sup>46</sup> *ibid.*

<sup>47</sup> European Union Agency for Fundamental Rights, '#BigData: Discrimination in data-supported decision making' (2018).

<sup>48</sup> GDPR art 22.

<sup>49</sup> European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust COM (2020) 65 final.

<sup>50</sup> European Commission, Regulatory framework proposal on Artificial Intelligence <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> accessed 24 September 2021.

The human rights approach is necessary to safeguard non-negotiable fundamental rights and detach them from risk assessments. This section uses examples found in the proposed Act to prove that adopting a human rights stance would have a different outcome compared to technology neutral and risk-based regulation. An idea underlying all the below-mentioned examples is that AI applications that cannot be used in compliance with human rights law should be explicitly banned. The proposed Act ignores this element by leaving the margin open in a few instances.

The first instance relates to the omission of banning automated weapons. The existence of technology neutrality addresses this technology and makes it subject to any rules or provisions included in this piece of legislation. However, autonomous weapons are received with great scepticism by the public, even referred to as ‘Killer Robots’<sup>51</sup>. Their use implies great human rights implications. So much so, that a significant body of research focuses on creation of new laws on fully autonomous weapons<sup>52</sup> or even their international prohibition<sup>53</sup>. On the authoritative spectrum, the European Parliament’s Committee on Foreign Affairs considers that the IHL principle of humanity should be the minimum admissibility standard for the use of AI-enabled systems in warfare<sup>54</sup>. This international principle forbids the infliction of ‘all suffering, injury or destruction not necessary for achieving the legitimate purpose of a conflict’<sup>55</sup>. Though the use of autonomous lethal weapons here is conceptualized within the context of conflict, hence extreme, it is used to illustrate how destructive such technology can be. The omission of its strict prohibition in the proposed Act proves that a human rights lens should be guiding any future regulatory efforts directed towards AI.

A second and very similar example is the omission of banning biometric mass surveillance in public areas. This omission has given rise to reactions from the data protection community, including a joint opinion from the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), which commented on the risk-based approach towards AI systems present in the proposal. In particular, the opinion stated that the concept of risk to fundamental rights should be aligned with the GDPR<sup>56</sup>. Pursuant to the GDPR, the processing of biometric data for the purpose of uniquely identifying natural persons is prohibited<sup>57</sup>.

---

<sup>51</sup> Brian Stauffer, ‘Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control’ (Human Rights Watch 2020) <<https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and>> accessed 16 September 2021.

<sup>52</sup> Bonnie Docherty, ‘The Need for and Elements of a New Treaty on Fully Autonomous Weapons’ (*Human Rights Watch*, 1 June 2020) <<https://www.hrw.org/news/2020/06/01/need-and-elements-new-treaty-fully-autonomous-weapons>> accessed 23 September 2021.

<sup>53</sup> Peter Asaro, ‘On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making’ (2012) 94 *International Review of the Red Cross* 687 <[https://www.cambridge.org/core/product/identifier/S1816383112000768/type/journal\\_article](https://www.cambridge.org/core/product/identifier/S1816383112000768/type/journal_article)> accessed 23 September 2021.

<sup>54</sup> European Parliament, Report on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)).

<sup>55</sup> International Committee of the Red Cross, ‘What Is IHL?’ <<https://www.icrc.org/en/document/what-ihl>> accessed 23 September 2021.

<sup>56</sup> EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

<sup>57</sup> GDPR art 9(1).



Examples of facial recognition systems analyzing biometric data include lie detectors and smart border control, predictive screening of public spaces to identify potential terrorist threats and the analysis of customers' emotions while shopping focused on either the goods or their arrangement within the shop<sup>58</sup>. Besides the EDPB and the EDPS, forty-four civil society organizations call for a ban on biometric mass surveillance alongside European Digital Rights (EDRi)<sup>59</sup>. Considering the public outcry underlining the possibility of real-time public surveillance, as well as its prohibition in the GDPR, it is only just that the Artificial Intelligence Act reflects on the issue on a similar human rights-focused manner.

The Proposal addresses AI systems with a risk-based approach instead of a human-rights approach. Instead of prohibiting the use of certain AI systems, it solely addresses them in the annex. This also reflects the principle of technology neutrality, because it is apparent that the regulators aim for including a vast variety of systems notwithstanding the possibility of other systems being equally as high-risk, however this is done in an open-ended manner. For purposes of clarifying that these systems are intrusive and shall not be used due to their effect on fundamental rights, employing a human rights lens would dictate for the explicit prohibition of these systems. Considering the structure of the Proposal, this could take place under Article 5. This change could protect human rights in a manner equal to the Universal Convention on Human Rights. An (extreme) analogy to this prohibition clause could be the prohibition of torture.

A noteworthy recommendation made by the EPDS and EDPB joint opinion deals with Article 57(4) of the proposal, which dictates the exchange between the Board, Union bodies, offices, agencies, and supervisory groups<sup>60</sup>. The Fundamental Rights Agency is recommended as becoming one of the Board's observers. This can allow constant oversight to the relevant mechanisms and actors, to ensure that fundamental rights are respected and abided by. Due to AI being such a vastly violating technology, it is indeed necessary that its interaction with human rights is assessed on a case-by-case basis.

## V. Concluding remarks

With the emergence of AI presence in society and its functioning, the relationship between AI and human rights is becoming increasingly tense. Though AI is perceived as an improvement of modern society, it challenges fundamental rights like no other technological moment in history of humankind.

Technology neutrality is a valuable principle to be observed when regulating because it saves a lot of future work and allows a margin of freedom for self-regulation and co-regulation. The

---

<sup>58</sup> European Data Protection Supervisor, 'Facial Emotion Recognition' (2021) <[https://edps.europa.eu/system/files/2021-05/21-05-26\\_techdispatch-facial-emotion-recognition\\_ref\\_en.pdf](https://edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf)> accessed 23 September 2021.

<sup>59</sup> European Digital Rights (EDRi), 'Ban Biometric Mass Surveillance!' (*European Digital Rights (EDRi)*) <<https://edri.org/our-work/blog-ban-biometric-mass-surveillance/>> accessed 23 September 2021.

<sup>60</sup> EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) 17.

GDPR proves that such regulation could be beneficial. The combination of a technology neutrality with a risk-based approach in AI regulation policies is the issue. The Artificial Intelligence Act is a beacon illustrating that change needs to occur to achieve ultimate safeguarding of fundamental rights without negating factors. Therefore, a risk-based lens and the approach of technologies in a neutral manner does not guarantee protection for individuals, data subjects, consumers.

This essay proposes that adopting a human rights lens can enhance protection and align new regulation with existing human rights legislation. To align the proposal with human rights, changes need to be tangible, such as the ones proposed. After all, it is time that we stop referring to AI as something external and self-evolving and start considering that humans develop and use it for their own advantage. The Fourth Industrial Revolution blurs boundaries between the physical, digital, and biological worlds, but it does not need to diminish fundamental values and rights vis-à-vis technological change. Thus, the ultimate goal of AI policy makers and regulators should be to protect fundamental rights before anything else.

\*\*\*

## Bibliography

Winston James Maxwell and Marc Bourreau, 'Technology Neutrality in Internet, Telecoms and Data Protection Regulation' [2014] SSRN Electronic Journal <<http://www.ssrn.com/abstract=2529680>> accessed 24 September 2021.

'EU: New Proposal on Artificial Intelligence Must Protect Human Rights' (*ARTICLE 19*, 2021) <<https://www.article19.org/resources/eu-artificial-intelligence-and-human-rights/>> accessed 23 September 2021.

Alessio Azzutti, Wolf-Georg Ringe and H Siegfried Stiehl, 'Machine Learning, Market Manipulation and Collusion on Capital Markets: Why the "Black Box" Matters' [2021] SSRN Electronic Journal <<https://www.ssrn.com/abstract=3788872>> accessed 16 September 2021.

Teresa Rodríguez de las Heras Ballell, 'Legal Challenges of Artificial Intelligence: Modelling the Disruptive Features of Emerging Technologies and Assessing Their Possible Legal Impact' (2019) 24 Uniform Law Review 302 <<https://academic.oup.com/ulr/article/24/2/302/5526861>> accessed 16 September 2021.

Asaro P, 'On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making' (2012) 94 International Review of the Red Cross 687 <[https://www.cambridge.org/core/product/identifier/S1816383112000768/type/journal\\_article](https://www.cambridge.org/core/product/identifier/S1816383112000768/type/journal_article)> accessed 23 September 2021.

Baweja S and Singh S, 'Beginning of Artificial Intelligence, End of Human Rights' (*LSE*) <<https://blogs.lse.ac.uk/humanrights/2020/07/16/beginning-of-artificial-intelligence-end-of-human-rights/>> accessed 23 September 2021.

Briglaue W, Stocker V and Whalley J, 'Public Policy Targets in EU Broadband Markets: The Role of Technological Neutrality' (2020) 44 Telecommunications Policy 101908 <<https://linkinghub.elsevier.com/retrieve/pii/S0308596119304549>> accessed 16 September 2021.

Charter of Fundamental Rights of the European Union [2012] OJ C326/391 (hereinafter 'the Charter').

Choubey S, Goswami P and Gautam S, 'AI Based Sustainable Approach for Metal Extraction from E-Waste: A Comprehensive Literature Review', *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (IEEE 2020) <<https://ieeexplore.ieee.org/document/9316121/>> accessed 16 September 2021.

Cooley M, 'The Myth of the Moral Neutrality of Technology' (1995) 9 AI & Society 10 <<http://link.springer.com/10.1007/BF01174475>> accessed 16 September 2021.

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 [1950] ETS 5.

Docherty B, 'The Need for and Elements of a New Treaty on Fully Autonomous Weapons' (*Human Rights Watch*, 1 June 2020) <<https://www.hrw.org/news/2020/06/01/need-and-elements-new-treaty-fully-autonomous-weapons>> accessed 23 September 2021.

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Fostering a European approach to Artificial Intelligence COM (2021) 205 final.

European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG), 'A Definition of AI: Main Capabilities and Scientific Disciplines' (2018).  
European Digital Rights (EDRi), 'Ban Biometric Mass Surveillance!' (*European Digital Rights (EDRi)*) <<https://edri.org/our-work/blog-ban-biometric-mass-surveillance/>> accessed 23 September 2021.

European Commission, Regulatory framework proposal on Artificial Intelligence <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> accessed 24 September 2021.

European Parliament, Report on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)).

European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust COM (2020) 65 final.

European Union Agency for Fundamental Rights, '#BigData: Discrimination in data-supported decision making' (2018).

Fisher DH, 'Computing and AI for a Sustainable Future' (2011) 26 IEEE Intelligent Systems 14 <<http://ieeexplore.ieee.org/document/6096574/>> accessed 16 September 2021.

Gibbs S, 'Women Less Likely to Be Shown Ads for High-Paid Jobs on Google, Study Shows' *The Guardian* (8 July 2015) <<https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study>> accessed 23 September 2021.

Halfteck G, 'Legislative Threats' (2008) 61 *Stanford Law Review*.

Hildebrandt M and Tielemans L, 'Data Protection by Design and Technology Neutral Law' (2013) 29 *Computer Law & Security Review* 509 <<https://www.sciencedirect.com/science/article/pii/S0267364913001313>> accessed 23 September 2021.

International Committee of the Red Cross, 'What Is IHL?' <<https://www.icrc.org/en/document/what-ihl>> accessed 23 September 2021.

Keyes O, Hutson J and Durbin M, 'A Mulching Proposal' [2019] arXiv:1908.06166 [cs] <<http://arxiv.org/abs/1908.06166>> accessed 23 September 2021.

Lampo A, Mancarella M and Piga A, '(Non)-Neutrality of Science and Algorithms: Machine Learning between Fundamental Physics and Society' [2020] arXiv:2006.10745 [physics] <<http://arxiv.org/abs/2006.10745>> accessed 16 September 2021.

Leenes R and others, 'Regulatory Challenges of Robotics: Some Guidelines for Addressing Legal and Ethical Issues' (2017) 9 *Law, Innovation and Technology* 1 <<https://doi.org/10.1080/17579961.2017.1304921>> accessed 23 September 2021.

Liao H-T and Wang Z, 'Sustainability and Artificial Intelligence: Necessary, Challenging, and Promising Intersections', *2020 Management Science Informatization and Economic Innovation Development Conference (MSIED)* (IEEE 2020) <<https://ieeexplore.ieee.org/document/9382599>> accessed 16 September 2021.

Maas MM, 'Aligning AI Regulation to Sociotechnical Change' [2021] *SSRN Electronic Journal* <<https://www.ssrn.com/abstract=3871635>> accessed 16 September 2021.

Maxwell W, 'Technology Neutrality in Internet, Telecoms and Data Protection Regulation' (*Hogan Lovells Global Media and Communications Watch*, 17 November 2014) <<https://www.hlmediacomms.com/2014/11/17/technology-neutrality-in-internet-telecoms-and-data-protection-regulation/>> accessed 16 September 2021.

McGregor L, Murray D and Ng V, 'INTERNATIONAL HUMAN RIGHTS LAW AS A FRAMEWORK FOR ALGORITHMIC ACCOUNTABILITY' (2019) 68 *International and Comparative Law Quarterly* 309 <[https://www.cambridge.org/core/product/identifier/S0020589319000046/type/journal\\_article](https://www.cambridge.org/core/product/identifier/S0020589319000046/type/journal_article)> accessed 21 September 2021.

Mercier-Laurent E, 'What Technology for Efficient Support of Sustainable Development?' (2015) <<https://fedcsis.org/proceedings/2015/drp/010.html>> accessed 16 September 2021.

Mijatović D, 'Safeguarding Human Rights in the Era of Artificial Intelligence' (*Council of Europe Portal*, 2018) <<https://www.coe.int/en/web/commissioner/blog/>>

[/asset\\_publisher/xZ32OPEoxOkq/content/safeguarding-human-rights-in-the-era-of-artificial-intelligence](#)> accessed 23 September 2021.

Murillo Arias J, 'What Should Be Taken into Account If Artificial Intelligence Is to Be Regulated?' (*Finextra Research*, 26 October 2020) <<https://www.finextra.com/the-long-read/62/what-should-be-taken-into-account-if-artificial-intelligence-is-to-be-regulated>> accessed 21 September 2021.

Pejčinović Burić M, 'Artificial Intelligence and Human Rights' (*Council of Europe Portal*) <<https://www.coe.int/en/web/artificial-intelligence/secretary-general-marija-pejcinovic-buric>> accessed 23 September 2021.

Popkova EG and Sergi BS (eds), *Scientific and Technical Revolution: Yesterday, Today and Tomorrow*, vol 129 (Springer International Publishing 2020) <<http://link.springer.com/10.1007/978-3-030-47945-9>> accessed 16 September 2021.

Reed C, 'Taking Sides on Technology Neutrality' (2007) 4 SCRIPT-ed 263 <<http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp>> accessed 17 September 2021.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2016 L 119/1.

Risse M, 'Human Rights and Artificial Intelligence: An Urgently Needed Agenda' (2019) 41 Human Rights Quarterly 1 <<https://muse.jhu.edu/article/716358>> accessed 21 September 2021.

Singer N and Metz C, 'Many Facial-Recognition Systems Are Biased, Says U.S. Study' *The New York Times* (19 December 2019) <<https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html>> accessed 23 September 2021.

Stauffer B, 'Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control' (Human Rights Watch 2020) <<https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and>> accessed 16 September 2021.

Taddeo M and Floridi L, 'How AI Can Be a Force for Good' (2018) 361 *Science* 751 <<https://www.sciencemag.org/lookup/doi/10.1126/science.aat5991>> accessed 21 September 2021.

UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III).