ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

17 GENNAIO 2022

federalismi.it

Special issue No. 2/2022

Non-State Actors and Human Security in Navigable Spaces

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

ISSN 1826-3534
Numero 2, 2022
Tutti i contributi, ad eccezione dell'editoriale di apertura, sono stati sottoposti a *double blind peer review*.

Direttore responsabile: Prof. Annamaria Poggi

Vice Direttore responsabile: Prof. Federica Fabrizzi

Comitato di direzione: Prof. Luisa Cassetti; Prof. Marcello Cecchetti; Prof. Carlo Curti Gialdino; Dott. Renzo Dickmann; Dott. Antonio Ferrara; Prof. Tommaso Edoardo Frosini; Prof. Diana Urania Galetta; Prof. Roberto Miccù; Prof. Andrea Morrone; Prof. Giulio M. Salerno; Prof. Maria Alessandra Sandulli; Prof. Sandro Staiano.

Redazione: dott. Federico Savastano (Redattore Capo); dott. Francesco Battaglia; Prof. Cristina Bertolino; Prof. Tanja Cerruti; dott. Caterina Domenicali; dott. Giovanni Piccirilli; Prof. Massimo Rubechi; Prof. Martina Sinisi; Prof. Alessandro Sterpa.

Segreteria di redazione: dott. Simone Barbareschi; dott. Lucio Adalberto Caruso; dott. Adriano Dirri; dott. Luisa Giurato; dott. Eleonora Iannario; dott. Ekaterina Krapivnitskaya; dott. Nicola Pettinari; dott. Giulia Renzi; dott. Francesco Severa; dott. Sergio Spatola.

E-mail: redazione@federalismi.it

Table of contents

Business and Human Rights in the Age of Artificial Intelligence*

by Marco Fasciglione
PhD Researcher of International Law
at CNR

Abstract [En]: While the development and the utilization of artificial intelligence (AI) open many possibilities to explore its benefits to societies, they are also potentially capable to have negative impacts on the enjoyment of internationally recognised human rights. This paper argues that the establishment of a regulatory regime on AI technology, based upon 'human rights by design' approach, should look at the international framework on business and human rights with its emphasis on the duty to protect pending on States as well as on the responsibility to respect human rights, with its human rights due diligence duty, pending on the corporate sector.

Abstract [It]: Se, da un lato, lo sviluppo e l'utilizzo dell'intelligenza artificiale (IA) possono comportare benefici per la società, essi sono anche potenzialmente in grado di avere impatti negativi sui diritti umani riconosciuti nei diversi strumenti internazionali. Il presente articolo suggerisce che la creazione di un quadro regolamentare applicabile allo sviluppo e all'utilizzo dell'Intelligenza Artificiale, dovrebbe essere fondato su di un approccio 'human rights by design' e utilizzare a tal fine il quadro internazionale su impresa diritti umani, con la sua enfasi sull'obbligo di proteggere che pende sugli Stati e sulla responsabilità di rispettare, con il connesso dovere di due diligence sui diritti umani, che pende sulle imprese.

Keywords: AI; companies; UN Guiding Principles on Business and Human Rights; Human Rights by Design; Corporate Human Rights Due diligence
Parole chiave: IA; imprese; Principi Guida ONU su imprese e diritti umani; human rights by design; due diligence aziendale sui diritti umani

1. Introduction

Machine learning, algorithms and other Artificial Intelligence (AI) applications are increasingly imbuing almost every sort of human activity.[1] The impacts of the development of this technology are everywhere

* Articolo sottoposto a referaggio. I would like to thank the anonymous reviewers for their suggestions and comments. I am also indebted to Angelica Bonfanti (University of Milan) and Chiara Macchi (Wageningen University and Research) for providing critical insights and constructive remarks as well as for keeping a keen eye on the coherence among the different parts of the text. Of course, any remaining flaw is the sole responsibility of the author.

[1] There is not universally accepted definition of AI. Rather than referring to concrete applications, it reflects recent developments that encompass a variety of technological processes enabling machines to act intelligently and thus to replace humans in performing a number of activities. From this side the expression is generally used as an umbrella concept. According to the OECD "an Artificial Intelligence (AI) System is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments" (see OECD, Recommendation of the Council on Artificial Intelligence, 2019). The EU High-Level

and present both positive effects and challenges for the lives of the people. On the one side, AI and machine learning have opened up new opportunities for productivity, economic development, and advancement in various sectors, from healthcare to agriculture. On the other one, however, its rapid and unregulated development as well as its pervasiveness in modern society pose risks to human rights and are even reshaping the public debate concerning the relationships between technology and democracy and how these relationships should be framed in order to prevent negative human rights impacts from algorithmic decision-making processes. Under the first aspect, in effect, the development of such technologies can be beneficial to the protection of human rights due to their positive impact, *inter alia*, on women rights, on the right to health, on the rights of the elderly, as for instance by assisting elders to perform tasks they are no longer able or willing to perform and allowing them to "fully exercise their human rights on an equal basis with others".[2] Also, it may unlock significant improvements in occupational health and safety through automation of dangerous tasks: the use of AI in smart grids, smart cities and connected devices can help, indeed, to reduce greenhouse gas emissions and aid in the adaptation to climate change. Under the second aspect, the capabilities of AI, based on big data and combined with the pervasiveness of devices and sensors of the Internet of Things, will eventually govern core functions of society, reaching from education via health, science and business right into the sphere of law, security and defence, political discourse and democratic decision making. In this respect, the use of algorithms and machine learning is potentially capable to put in crisis the "Trinitarian formula" that is at the core of Western, liberal constitutions in its being based on the triad of human rights, democracy and the rule of law.[3] This causes human rights concerns across a wide range of sectors. For instance, if applied for predictive policing, surveillance or judicial decision-making, these technologies may amplify current societal bias and interfere with many human rights guarantees, including, but not limited to, non-

Expert Group on Artificial Intelligence (AI HLEG) defines AI as referring to "systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)" (see AI HLEG, A definition of AI: Main capabilities and disciplines, 2019). This definition is also applied by the European Union Agency for Fundamental Rights (FRA) in its reports (see FRA, *Getting the future right. Artificial intelligence and fundamental rights*, 2020, at p. 19).

[2] See HRC, Report of the Independent Expert on the Enjoyment of All Human Rights by Older Persons (21 July 2017) UN Doc A/HRC/36/48, para 89; other examples of positive impact of AI are described in: FRA, *Fundamental Rights Report*, 2020, pp. 148-149.

[3] See M. KUMM, *The Cosmopolitan Turn in Constitutionalism: An Integrated Conception of Public Law*, in Indiana Journal of Global Legal Studies, vol. 20, 2013, pp. 605-628, at 609. On the role played by these intersecting notions in and for international law see Id., *Constituent power, cosmopolitan constitutionalism, and post-positivist law*, in International Journal of Constitutional Law, 14, 2016, pp. 697-711. For an international human rights law analysis, see G. DELLA MORTE, *Les tensions détectables entre le recours aux Big Data et les normes internationales à protection des droits de l'homme*, in J. ILIOPOULOS-STRANGAS, E. LEVITS, M. POTACS, J. ZILLER (ed.), *Die Herausforderungen der digitalen Kommunikation für den Staat und seine demokratische Staatsform*, Nomos Verlagsgesellschaft, Baden Baden 2021, 165-175.

discrimination, due process, the right to privacy and the right to freedom of speech and expression.[4] Algorithm-based business models, such as digital labour platforms, can reproduce societal biases, thus intruding upon the right to be free from discrimination in respect to the access to work. A noteworthy example of such an impact is provided by the algorithm (the so-called 'Frank algorithm') utilized by the company Deliveroo Italia in order to manage the digital booking system of the working sessions of riders employed by the company. The algorithm, indeed, who was supposed to establish the priority according to which riders had to choose their working sessions, determined each rider's score on the basis of two parameters: reliability and participation. The mechanism was designed in such a way to penalise workers who were unjustifiably absent from working sessions they had been assigned, but, unfortunately, it did not perform any differentiation for those situations involving legitimate abstention, such as the exercise of the right to strike.[5] Algorithmic systems can also lead certain individuals to be erroneously qualified as potential threats or terrorists with the risk to expose them to violations of the right not to be arbitrarily arrested, in case they are subject to pre-trial detention, or to a violation of the right to life, in case they are killed by military drones, or other lethal autonomous weapons systems (LAWS), in the attempt to prevent a terrorist attacks.[6] In the same vein, the absence of such framing for the Internet economy has already led to a widespread culture of disregard of the law and put democracy in danger, the *Facebook Cambridge Analytica* scandal being only the latest warning in that respect.[7]

Simply put, in a global digital environment, the threats for rule of law, human rights and democracy "do not just come from the implementation of algorithmic technologies by public actors but also, and primarily, from the ability of transnational private actors to develop and enforce private standards competing with public values".[8] Accordingly, the need there exists to clarify how to support the

[4] See FRA, *Getting the future right*, cit., pp. 57-86.

[5] The case has given rise to a court action filed by some Italian labor unions against the company. On 31 December 2020, the Bologna District Court handed down its decision sentencing Deliveroo Italia for discriminatory conduct in respect to the functioning of the algorithm in the digital platform (see Bologna District Court, Filcams Cgil Bologna, Nidil Cgil Bologna, Filt Cgil Bologna c. Delveroo Italia S.r.l., 31 December 2020). The operative modalities of the algorithm have been also challenged by the Italian data protection authority (DPA) who ordered in July 2021, Deliveroo Italy to pay a fine of EUR 2.5 million due to non-transparent use of algorithms and disproportionate collection of workers' data. The authority found violations of some provisions of the General Data Protection Regulation, the national privacy legislation and legislation protecting the workers, such as the Workers' Statute (see the DPA, *injuction order against Deliveroo s.r.l.*, 22 luglio 2021).

[6] As far as a recent US drone strike in Afghanistan, see The New York Times, *Times Investigation: In U.S. Drone Strike, Evidence Suggests No ISIS Bomb,* 10 September 2021, updated 2 October 2021. As to the debate on the legal implications of the use of LAWS, see *inter alia* A. SPAGNOLO, *Human Rights Implications of Autonomous Weapon Systems in Domestic Law Enforcement: Sci-fi Reflections on a Lo-fi Reality*, in Questions of International Law, Zoom-in 43, 2017, pp. 33-58.

[7] The case concerns the company Cambridge Analytica harvesting of data of millions of Facebook's users without their consent and them utilization to interfere with the 2016 presidential elections in the United States. On this issue see D. DESIERTO, *Human Rights in the Era of Automation and Artificial Intelligence*, in EJIL:Talk!, 26 February 2020.

[8] See O POLLICINO, G. DE GREGORIO, *Constitutional Democracy in the Age of Algorithms: The Implications of Digital Private Powers on the Rule of Law in Times of Pandemics*, in MediaLaws, 11 november 2020; Id., *The Principle of the Rule of Law*

maintenance or, even better, the strengthening of that constitutional 'Trinitarian formula', rather than letting it be weakened by these new powers capable of infringing on the basic rights of human beings.[9] In this respect, the international framework on business and human rights already offers a baseline from which to start in order to address human rights risks associated to the development and utilization of AI technology by the corporate sector. This paper aspires to review the applicability of this international framework in relation to corporate business operations developing AI and machine learning technologies, by highlighting the duties pending respectively on States and on the private sector.[10]

2. The relevance of Business and Human Rights in the contemporary AI debate

A decade ago, the late Prof. John Ruggie, the architect of the UN Guiding Principles on Business and Human (UNGPs),[11] highlighted how "the root cause of the business and human rights predicament today lies in the governance gaps created by globalization – between the scope and impact of economic forces and actors, and the capacity of societies to manage their adverse consequences" and that it is precisely these governance gaps to "provide the permissive environment for wrongful acts by companies of all kinds without adequate sanctioning or reparation".[12] The parallels to the current nature and speed of technological development and the potential negative impact stemming from ICT corporate activities are self-evident. Consider the following hypothetical scenario.

A large company who offers services and products to the final market decides to integrate an AI into its business processes with the purpose to optimize the business and increase its profits. Let's imagine, by way of example, a multinational company from the automotive sector selling vehicles for transporting goods and people. Services and products sold by the company may include: cars, vans, trucks and trailers, the spare parts, the power supply solutions these vehicles use, and even the financing solutions for purchasing each vehicle (through financial institutions managed or participated in by the leading company) and the whole chain of suppliers and sub-suppliers scattered around the world. What if, in performing its tasks, the AI would be authorized to interact across the entire automotive supply chain?

in the Regulation of AI, in PABLO GARCÍA MEXÍA and FRANCISCO PÉREZ BES (eds), *Artificial Intelligence and the Law*, Wolters Kluwer, Madrid, 2021.

[9] The Open Letter on AI of 2015, signed by major scientists and business people, has generated an intensive debate on how to regulate AI and how to avoid potential pitfalls attributed to the mismanagement of this technology. See M. SPARKES, Top Scientists Call for Caution over Artificial Intelligence, The Telegraph, 13 January 2015.

[10] On the contrary, the analysis will focus only incidentally on issues that are already largely investigated by the doctrine, such has privacy and data protection.

[11] Human Rights Council, *Human Rights and Transnational Corporations and Other Business Enterprises*, UN Doc. A/HRC/RES/17/4 of 7 July 2011.

[12] Human Rights Council, *Protect, Respect and Remedy: a Framework for Business and Human Rights Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie*, UN Doc. A/HRC/8/5 of 7 April 2008, para. 3.

In this case, the AI would have the possibility to exploit as much as possible every step of the supply chain to maximise profit. Even assuming that its designers had inserted a code of laws for each country where the company operates, it might be able to find 'creative' solutions to 'evade' the code: from the creation of sophisticated shell companies to avoid paying taxes (to the detriment of the countries where the multinational operates and in which it should pay taxes), to strategies of purchasing resources (raw materials, research personnel, etc.) paying them as little as possible, activating production processes that, although not necessarily illegal (depending on the country), could result in damage to the environment, people and entire economies. Indeed, that labour legislations in Asia are different from those in the Western Countries, with the former that may have different (in some cases, broader) parameters than in the latter, is a truism. An unscrupulous AI, then, while formally respecting local laws, could re-plan the entire supply chain of the hypothetical automotive company by moving production where is 'more convenient'. And this only with the purpose to maximise profit. If this situation is not a novelty for contemporary business models, where the principle of the shareholder primacy compels companies to take advantage of the opportunity granted by the mechanisms of production along the global supply chains in order to reduce costs and maximise profits, a highly evolved AI might push this path to its extreme consequences in an inevitable scalar effect, with devastating impacts for the planet and the whole society. It is in respect to such, and other similar, scenarios that the UNGPs framework may provide some regulatory-like solutions.

The UNGPs, it is well-known, are not a legally binding instrument. They may be regarded as a common global platform for action to secure human rights in the global economy based on three Pillars: *a*) the duty of States to protect against human rights by abuses by third parties, including business enterprises; *b*) the corporate responsibility to respect human rights; and *c*) the need for greater access by victims to effective judicial and non-judicial remedies.[13] Conceptually, the UNGPs are expression of an approach to regulation in the form of a principles-based exercise in polycentric governance. With the term "polycentric governance" Ruggie meant the way forward to systemically advance the cause of human rights in the global economy based on three concurring regulatory systems: public governance encompassing law and policy; corporate governance reflecting risk management; and civil governance reflecting social expectations of stakeholders. This approach stems directly from the acknowledgment that today human rights violations often occur in a context characterized by joint and coordinated, rather

[13] Despite their non-binding character, UNGPs constitute the first authoritative global standard on business and human rights. Actually, they have been internationally acknowledged and recognized by several States and the major international organizations and institutions, including the European Union and the Council of Europe, as a basis for the development of their own B&HR policies and standards. Bodies charged with policy-setting functions in human rights regional systems in Europe as well as in the Americas and in Africa have endorsed the Guiding Principles in the process of developing regional policy frameworks dealing with the negative effects on human rights of private sector activities.

than independent, actions from different duty-bearers, and that accordingly, in order to achieve better protection for individuals and communities against corporate-related human rights harm, each of these governance systems needs to be mobilized and put in compatible directions. In other terms, on the one hand, States owe a duty to protect human rights from violations occurring in the framework of business activities and they play a crucial role in controlling and supervising corporate activities. As far as AI technologies are concerned, States have a duty to ensure that the development of these technologies be not detrimental to human rights. On the other hand, enterprises, including hi-tech companies developing or deploying AI technologies, are urged to respect human rights in the course of their operations and throughout the entire value chain, and in particular by performing human rights due diligence. This means taking steps in order to prevent their business activities from having a negative impact on human rights and, if an impact is originated, to prevent, mitigate and remedy it.

3. State Obligations in Respect to Human Rights and AI

It is well-known that under international law by becoming parties to international human rights treaties[14] States assume obligations to respect, to protect and to fulfil human rights. The obligation to respect means that States must refrain from interfering with or curtailing the enjoyment of human rights. The obligation to protect requires States to protect individuals and groups against human rights abuses. The obligation to fulfil means that States must take positive action to facilitate the enjoyment of basic human rights. Simply put, this includes that from one side contracting States are duty-bound to abstain from unduly interfering with the enjoyment of human rights of individuals falling within their jurisdiction, and from another side they also bear positive obligations to secure human rights of everyone under their jurisdiction. While in the first case States have not to abridge the enjoyment of human rights through their actions or those of their organs or agents, in the second case they have to adopt all reasonable and appropriate steps in protecting individuals against violations of human rights, as for instance when perpetrated by non-state actors, including business enterprises.[15] This State duty to protect applies to all

[14] See, *inter alia*, at universal level the International Covenant on Civil and Political Rights (adopted 16 November 1966, entered into force 23 March 1976) and the International Covenant on Economic, Social and Cultural Rights (adopted 16 November 1966, entered into force 23 March 1976); at regional level the Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953), the Charter of Fundamental Rights of the European Union (adopted in 2000, and came into force in December 2009 along with the Treaty of Lisbon); the American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978), and the African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986).

[15] As to the State responsibility for violation of positive obligations, see R. PISILLO MAZZESCHI, *Responsabilité de l'Etat pour violations des obligations positives relatives aux droits de l'Homme*, in Recueil des Cours de l'Académie de Droit International de La Haye, t. 333 (2008), Martinus Nijhoff, Leiden/Boston, 2009.

recognized rights that private parties are capable of impairing on, and to all types of business enterprises,[16] extends to all organs of the State and requires that contracting Parties to international treaties take all measures that could reasonably be adopted to prevent the occurrence of human rights violations. It goes without saying, States are bound by this negative and positive obligations also when they are involved in the development or utilization of AI technologies that may intrude upon abovementioned rights,[17] and this since existing international human rights instruments "are applicable irrespective of contextual changes brought about by AI" and must be complied with to ensure that technological progress occurs in line with the principles of human rights, democracy and the rule of law.[18] Summing up, States maintain their positive and negative obligations under international human rights law in the context of AI with the consequence that they have to refrain from using AI technology, and prevent third parties, including Hi-tech companies, from using it, in a way that unduly interferes with human rights, such as the right to freedom of opinion, the right to freedom of expression, the right to privacy, the right to an effective remedy and the principle of non-discrimination.[19]

Violations of such obligations may entail the international responsibility of the State. It is well-known that a State may incur international responsibility where a corporation's conduct may be attributed to the State itself. In respect to the conduct of companies using or developing AI technologies, this may occur, for instance, if the company is empowered by the State to exercise functions of public nature normally attributed to State organs, such as law enforcement or judicial decision making.[20] Some of the most problematic uses of AI-systems, indeed, concern applications deployed by the State while exercising important public functions, such as the application of automated facial recognition by police forces, or the deployment of predictive AI-systems within the judiciary to assess an individual's potential for recidivism. These issues, as for instance, have been at the heart of a pioneering Dutch ruling handed down in 2020 by the commercial section of the Hague District Court. The District Court stated that the secret 'SyRI' algorithm used by the Dutch authorities to predict if and which person would be most at risk of committing public housing or social security fraud, was contrary to the right to respect for private

[16] See UNHRC, *Business and human rights: Towards operationalising the 'protect, respect, remedy' framework*, *Report of the UNSRSG on the issue of human rights and transnational corporations and other business enterprises, John Ruggie*, UN Doc. A/HRC/11/13, April 22, 2009, para. 13.

[17] See General Assembly, *Promotion and protection of the right to freedom of opinion and expression, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc A/73/348, 29 August 2018, para 19.

[18] Council of Europe, *Conclusions from the Conference 'Governing the Game Changer. Impacts of Artificial Intelligence on Human Rights, Democracy and the Rule of Law', 26-27 February 2019*, para. 11.

[19] General Assembly, *Promotion and protection of the right to freedom of opinion and expression, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, cit.

[20] As for instance, Art. 5 of the 2001 Draft Articles on Responsibility of State for Internationally Wrongful Acts would be applicable where machine learning installed by private companies is used in the administration of justice. See ILC, *Draft Articles on Responsibility of State for Internationally Wrongful Acts*, *Yearbook of the International Law Commission*, 2001, vol. II (Part 2), art. 5.

and family life, as enshrined in Article 8(2) of the European Convention on Human Rights. Indeed, the algorithm was designed in order to compile the profiles of past offenders in order to achieve "offender patterns". From these patterns, the system tracked databases to identify which individuals were most likely to fit into these predetermined patterns and thus be more closely monitored. The District Court considered this profiling activity to be contrary to the right to privacy, since such monitoring was not justified by any other reason than the stigmatization consequent from the functioning of SyRI algorithm.[21] Conversely, the violation of human rights may be the result of a conduct undertaken by companies developing, or employing, AI technologies acting under "the instructions of, or under the direction and control of" the State. In this situation, which applies for example to State-owned and controlled companies, the latter may be held responsible, provided that there is evidence that it used its ownership in, or control of, the company to achieve a specific result.[22]

However, in the majority of cases the wrongful conduct arising from the development or deployment of AI technologies will not be normally attributable to a State. Yet, even where the conduct of a private person or entity cannot be attributed to a State, a State may nevertheless bear obligations of "due diligence" with respect to that conduct. Here, in effect, the abovementioned State obligation to protect individuals from interferences with their human rights caused by third parties, including private corporations, applies. As well-known, this obligation encompasses a due diligence duty and requires States to take appropriate steps to prevent, investigate, punish and provide remedial measures, including by means of legislation, regulation, or adjudication.[23] Rules on State responsibility, then, can play a substantial role in shaping of the primary legal obligations of a State with respect to private companies,

[21] This is the first time that a national court in Europe has outlawed the operation of an intelligent algorithm in the light of European fundamental rights law (see Rechtbank Den Haag, *Nederlands Juristen Comité Voor de Mensenrechten et al, vs The State of the Netherlands*, C/09/550982/HAZA18-388, of 5 February 2020). As to the literature on the impact of AI-systems in the judiciary, see O. POLLICINO, Judicial Protection of Fundamental Rights on the Internet, Hart Publishing, Oxford, 2021; G.M. RUOTOLO, *The End of Dormancy. Judicial Independence Through Data-Driven Knowledge and Artificial Intelligence in an International and European Law Perspective*, in S. SHETREET, H.E. CHODOSH, E. HELLAND (eds), *Justice Challenged: in pursuit of judicial independence*, Brill/Nijhoff, Leiden Boston, 2021, pp. 159-179.

[22] Art. 8 of the Draft Articles on Responsibility of State for Internationally Wrongful Acts would be applicable to these circumstances. It is worth recalling that under international law States are not generally directly responsible for the acts or omissions of State-owned or State-controlled companies. This is due to the fact that international law acknowledges the general separateness of corporate entities at the national level, except in those cases where the "corporate veil" is a mere device or a vehicle for fraud or evasion. See ILC, *Draft Articles on Responsibility of State for Internationally Wrongful Acts*, *Yearbook of the International Law Commission*, 2001, vol. II (Part 2), Art. 8, Commentary para. 6.

[23] This obligation is upheld in Principle 1 of the UNGPs. It reproduces, therefore, a traditional principle, which is part of the international human rights regime's very foundation, and which is applied by the most important international and regional human rights protection systems and mechanisms, including the ECtHR. On this specific point, see M. FASCIGLIONE, *Enforcing the State Duty to Protect under the UN Guiding Principles on Business and Human Rights: Strasbourg views*, in A. BONFANTI (ed.), *Business and Human Rights in Europe: International Law Challenges*, Routledge, New York and London, 2019, pp. 37-47; E. FURA-SANDSTROM, *Business and Human Rights – who cares?*, in L. CAFLISH ET AL. (eds.), *Liber amicorum Luzius Wildhaber: Human rights- Strasbourg views*, Engel, Kehl, 2007, pp. 159-176.

including those it has itself contracted and those operating on its own territory or on the territory it controls.

This observation leads us to a second kind of issue, a crucial one in respect to the regulatory attempts over AI companies: what is the jurisdictional scope of the State's obligations? Indeed, as a general rule, human rights treaties require contracting Parties to ensure and respect human rights within their jurisdiction. Yet the utilization of AI and other machine learning technologies is a typical activity that crosses physical State borders, thus raising the question whether the individuals whose human rights are infringed do actually fall within the State's 'jurisdiction'. In particular, when AI technology is utilized across a space without defined borders – like the Internet and cyberspace – the traditional State jurisdiction paradigm risks falling short. In respect to these situations,[24] the case law and practice of international human rights monitoring bodies have disclosed an extensive approach, admitting the extraterritorial application of the relevant human rights treaties any time the State exercises power or effective control over a foreign territory or individuals abroad. Interestingly, the Committee on economic social and cultural rights has endorsed this approach in respect to State obligations in the context of business activities in its General Comment No. 24. According to the Committee, indeed, States have an extraterritorial obligation to protect human rights which "extends to any business entities over which States parties may exercise control, in accordance with the Charter of the United Nations and applicable international law".[25] Comparable views may be found in the case law of the Committee on the Rights of the Child,[26] as well as of other human rights treaty bodies. While Principle 2 of the UNGPs, ignores these

[24] A bulk of literature exists on this issue, see among others P. DE SENA, "Juridiction étatique et imputation des violations extraterritoriales des droits de l'homme: Quelques observations", in D. ALLAND, V. CHETAIL, O. DE FROUVILLE, J. E. VIÑUALES (Eds.), *Unité et diversité du droit international/ Unity and Diversity of International Law. Écrits en l'honneur du Professeur Pierre-Marie Dupuy/Essays in Honour of Professor Pierre-Marie Dupuy*, 2014, Brill-Nijhoff, Leiden-Boston, pp. 785-801; M. MILANOVIC, Extraterritorial Application of Human Rights Treaties: Law, Principles and Policy, Oxford University Press, Oxford, 2011; O. DE SCHUTTER, International Human Rights Law: Cases, Materials, Commentary, Cambridge University Press, Cambridge, 2010, p. 162; F. COOMANS, M. KAMMINGA (eds.), Extraterritorial Application of Human Rights Treaties, Intersentia, Antwerp-Oxford, 2004; T. MERON, *Extraterritoriality of Human Rights Treaties*, in American Journal of International Law, 1995, pp. 78 ff.

[25] See CESCR, *General comment No. 24 on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities*, UN Doc. E/C.12/GC/24 of 10 August 2017, para. 31. In the literature see: M. FERRI, *The General Comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities*, in Federalismi, Focus Human Rights, 3, 2017, pp. 1-36. The Committee has also addressed specific extraterritorial obligations of States Parties concerning business activities in other General Comments, such as those relating to the right to water (*General Comment No. 15 (2002), The right to water (arts. 11 and 12)*, UN Doc. E/C.12/2002/11 of 20 January 2003, paras. 31 and 33), the right to work (*General Comment No. 18 (2006): The right to work (art. 6)*, UN Doc. E/C.12/GC/18 of 6 February 2006, para. 52), or the right to just and favourable conditions of work (*General Comment No. 23 (2016) on the right to just and favourable conditions of work (art. 7)*, UN Doc. E/C.1/GC/23 of 27 April 2016, para. 70).

[26] Committee on the Rights of the Child, *General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*, UN Doc. CRC/C/GC/16 of 17 April 2013, paras. 43-44.

developments by adopting an 'agnostic' view,[27] further decisions, however, seem to indicate a different path in holding States responsible for human rights violations caused by the use of new technologies even when the affected individuals are not within that State's territory or under its effective control.

Actually, when in *Big Brother Watch v United Kingdom* the ECtHRs has been confronted with complaints by journalists and human-rights organisations in regard to a complex bulk interception of communications involving both the receipt of intercept material from foreign governments and intelligence agencies and the obtaining of communications data from communication service providers, it has not ruled out its 'jurisdiction' within the meaning of Article 1 of the Convention despite the interference with Article 8 stemming from the interception of communications by foreign intelligence services did not meet the criteria for attributing the conduct of foreign authorities performing the interceptions to the respondent State. Both the Chamber and the Grand Chamber, indeed, have agreed in acknowledging that the interference in the present case was lying "in the initial request and the subsequent receipt of intercept material, followed by its subsequent storage, examination and use by the intelligence services" of the respondent State.[28] *Mutatis mutandis*, in the American human rights regional system, the Inter-American Court of Human Rights has interpreted the notion of 'jurisdiction' under Article 1 of the ACHR as encompassing situations where contracting States exercise effective control over activities that cause harm, and consequent violations of human rights, outside their territory.[29] While the Inter-American Court developed this rule with reference to transboundary environmental damage, nothing seems to prevent its application to other sectors, including the utilization of AI technologies.

Despite few commentators still dispute that such a duty currently corresponds to positive law endowed with general reach,[30] the time is ripe for acknowledging that the State duty to protect human rights with its twofold dimensions, the preventive one (taking measures for preventing human rights violations by private actors) and the remedial one (taking measures for remedying human rights violations committed by private actors), is apt to be translated into a general obligation for the 'home State' to adequately control and regulate extraterritorial activities of their private sector. This obligation, expression of a

[27] Commentary to Principle 2 affirms that "at present States are not generally required under international law to regulate the extraterritorial activities of business domiciled in their territory and/or jurisdiction. Nor are they generally prevented from doing so, provided there is a recognized jurisdictional basis".

[28] See ECtHR, First Section, *Big Brother Watch and Others v The United Kingdom*, judgment 13 September 2018, paras. 419 ff.; ECtHR, Grand Chamber, *Big Brother Watch and Others v The United Kingdom*, judgment 25 May 2021, paras. 495 ff.

[29] See Inter-American Court of Human Rights, *The Environment and Human Rights (State Obligations in Relation to the Environment in the Context of the Protection and Guarantee of the Rights to Life and to Personal Integrity – Interpretation and Scope of Articles 4(1) and 5(1) of the American Convention on Human Rights)*, Advisory Opinion OC-23/17, 15 November 2017, para. 104.

[30] C. METHVEN O'BRIEN, *The Home State Duty to Regulate the Human Rights Impacts of TNCs Abroad: A Rebuttal*, in Business and Human Rights Journal, 2018, p. 47 ff.

'functional' criterion of jurisdiction,[31] emphasizes the role that the State duty to protect human rights may play in offering victims avenues for remedies in an increasingly interdependent world, where some territorial States may lack the will, or the power, to take action against corporations. As noted elsewhere,[32] in these situations, States merely limit themselves to impose duties on corporations falling within their jurisdiction although this may have extraterritorial impact. This 'functionalist' approach to States extraterritorial duty to protect appears a logic outcome of the process of change nowadays encompassing international legal system in which powerful States increasingly assert their power abroad in ways that affect the rights of individuals beyond their national borders.[33]

This having said, one cannot help but observe that States currently play only a marginal role in the development and deployment of AI technologies. Hi-tech companies, indeed, hold a monopoly over AI know-how and the AI market, as well. They are the most likely actors potentially capable to infringe on human rights when developing and using AI technology, and the main entities possessing the technical capabilities to recognise and prevent human rights abuses. Therefore, any effort to regulate the sector, also in respect to the protection of human rights, may not avoid rendering hi-tech companies entirely part of the 'game'.

4. 'Human Rights by Design': The Corporate Responsibility to Respect Human Rights of Hi-tech Companies

While companies using AI technology under traditional international law do not bear direct human rights obligations, the challenges posed by the development of AI technologies and the difficulties encompassing State regulation are increasingly leading to alternative approaches to hard regulation, traditionally based on legal norms, by emphasizing the role of private sector in the regulatory process.[34] The solution proposed by the UNGPs's second Pillar relies on the corporate responsibility to respect.

---

[31] In a large array of literature supporting this view see, *inter alia*, C. MACCHI, *With trade comes responsibility: the external reach of the EU's fundamental rights obligations*, in Transnational Legal Theory, 2020, pp. 409-435; V. MORENO-LAX, C. COSTELLO, *The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model*, in S. PEERS ET AL (eds), *Commentary on the EU Charter of Fundamental Rights*, Hart Publishing, 2014, pp. 1657-1683; D. AUGENSTEIN, D. KINLEY, *When human rights 'responsibilities' become 'duties': the extraterritorial obligations of states that bind corporations*, in S. DEVA, D. BILCHITZ (eds.), *Human Rights Obligations of Business*, 2013, Cambridge University Press, Cambridge, pp. 271-294; H. KING, *The Extraterritorial Human Rights Obligations of States*, in Human Rights Law Review, 2009, pp. 521-556; R. MCCORQUODALE AND P. SIMONS, *Responsibility beyond Borders: State Responsibility for Extraterritorial Violations by Corporations of International Human Rights Law*, in The Modern Law Review, 2007, pp. 598-625.

[32] See M. FASCIGLIONE, *Another Step on the Road? Remarks on the Zero Draft Treaty on Business and Human Rights*, in Diritti umani e diritto internazionale, 2018, pp. 629-661.

[33] B. VAN SCHAAK, *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change*, in International Law Studies, 2014, pp. 20-65.

[34] Alternative approaches to regulation may take different forms, from soft-law or self-regulation by the industry, to ISO standards, codes conducts or other multi-stakeholders initiatives. In general, on this issue see A. BERTOLINI, E.

Corporate responsibility to respect is a global standard of expected conduct for all business enterprises, including companies developing or using AI technologies. It does not entail binding legal obligations for companies and exists independently of States' abilities and/or willingness to fulfil their own human rights obligations, and furthermore does not diminish those State obligations. Corporate responsibility to respect is crystallized in the UNGPs statement that companies "should respect human rights".[35] The commitment to respect[36] implies that companies should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved. The concept of 'human rights impacts', is one the core features of the corporate responsibility to respect. Businesses, indeed, bear different degrees of responsibility for those adverse impacts they cause, contribute to, or to which they are "directly linked to… by their business relationships".[37] In particular, the UNGPs requires enterprises to *a*) avoid *causing* adverse human rights impacts through their own activities (both acts and omissions); *b*) avoid *contributing to* adverse human rights impacts through their own activities; and *c*) seek to prevent or mitigate adverse human rights impacts that are *directly linked to* their operations, products or services by their business relationships, even if they have not caused neither contributed to those impacts. According to the UNGPs an hi-tech company may cause an adverse impact where its activities (actions or omissions) on their own 'remove or reduce a person's (or group of persons') ability to enjoy a human right, *i.e.* where the company's activities are sufficient to result in harm. Companies may for example 'cause' an adverse human rights impact if their actions result in violations of the right to privacy, or where, as occurred in the abovementioned *Deliveroo* case, the design and the running of an algorithm-managed digital platform result in discriminatory access or user experience. Companies, can 'contribute to' an adverse impact when its activities (actions or omissions) are combined with those of other actors in ways that cause harm. Contribution occurs where hi-tech companies' actions and decisions, including in the course of product design, promotion, deployment, selling/licensing and oversight of use, facilitated or incentivized the user in such a way as to make the adverse human rights impact more likely. Finally, 'linkage' refers to situations where a company has not caused or contributed to an adverse human rights impact, but there is nevertheless a link between the operations, products or services of the technology

PALMERINI, Regulating Robotics. A Challenge for Europe, EU Parliament, Directorate General for Internal Policies, Workshop on Upcoming Issues of EU Law, 2014, p. 173 ff.

[35] UNGPs Principle 11.

[36] UNGPs Principle 16 requires that companies express this commitment in a formal "statement of policy", approved by senior levels, which is publicly available and reflected in policies and procedures of the company. Unilateral voluntary commitments from companies deploying AI technologies are an example of such statement of policy. This is the case as for instance of the adoption by Google, in June 2018, of its *Principles on AI*, in which the tech giant also committed not to pursue "technologies whose purpose contravenes widely accepted principles of international law on human rights" (see *Artificial Intelligence at Google: Our Principles*). In the same vein, Microsoft has adopted in 2019 its own *Principles for Responsible AI*.

[37] UNGPs Principle 13.

company and that impact through the company's business relationships. A situation of linkage may occur, as for instance, where a company has provided technology to an entity (another company or a government) and it, in the context of using this product or service, act in such a way that it causes (or is at risk of causing) an adverse impact.[38]

Of course, the corporate duty to address negative impact on human rights has direct relevance for the current AI framework.[39] UNGPs in describing the *ratione materiae* scope of the corporate responsibility to respect clarifies that it potentially applies to all internationally recognized human rights. Indeed, since business enterprises can have with their operations an impact on virtually the entire spectrum of internationally recognized human rights, then their responsibility to respect applies to all such rights. The content of the category of internationally recognized human rights has to be "understood, at a minimum", as those included in the International Bill of Human Rights as well as those included in the fundamental labour rights set out in the 1998 ILO Declaration on Fundamental Principles and Rights at Work.[40] In addition, and particularly relevant for the present analysis, is the circumstance that according to UNGPs some human rights may be at greater risk than others in particular *industries* or *contexts*: therefore, in presence of these settings companies have to pay "heightened attention".[41] Development of AI, algorithm processes and machine learning technologies, their practical utilization in civil and military automated machines, originate situations deserving *exactly* such a heightened attention: rather than authorize derogations from human rights standard, these situations, indeed, impose on corporate actors an increased level of attention, and therefore particular diligence, as far as the respect of human rights.

How to practically realize this objective? Answering this question led us to consider that international standards on business and human rights call for a 'human rights by design' approach. Indeed, companies already deploy very complex 'privacy by design' processes that integrate privacy considerations during they key milestone in product development. As well-known, privacy by design has been established as a standard in systems engineering in the mid-1990s and has since then evolved as common industry practice. Principles at the foundation of this practice include: being proactive rather than reactive by anticipating and preventing privacy invasive events before they happen; being embedded into the design and architecture of IT systems and business practices, not bolted on as an add-on, after the fact; and requiring architects and operators to keep the interests of the individual uppermost. In other terms,

[38] AI developers or deployers also have different remediation responsibilities depending on whether they cause, contribute to, or are linked to adverse human rights impacts by their operations, products, services, or business relationships (see Principle 22 of the UNGP).

[39] For an analysis concerning the banking sector see J. RUGGIE, Comments on Thun Group of Banks: Discussion Paper on the Implications of UN Guiding Principles 13 & 17 in a In a Corporate and Investment Banking Context, 21 February 2017.

[40] UNGPs Principle 12.

[41] See the Commentary to UNGPs Principle 12.

'privacy by design' encompasses a risk assessment approach to data protection based upon a duty of impact assessment.[42] As far as the development and utilization of AI technology is concerned, the challenge is to expand the already existing legal obligation of impact assessment when AI is processing personal data in the context of automated decision making,[43] to the point of encompassing a general duty to perform human rights risk assessment in respect to *any* internationally recognized human rights when AI technologies are under development or are being deployed.[44] This 'human rights by design' approach to AI may be easily incorporated in the corporate human rights due diligence' (HRDD): HRDD indeed is applicable also in respect to the negative impact on human rights stemming from activities of companies developing or deploying AI technologies.

5. Corporate Human rights Due Diligence in the AI sector

Under the international framework on business and human rights companies have to carry out human rights due diligence (HRDD) in order to identify, prevent, mitigate and account for how they address their adverse human rights impacts.[45] Therefore, in order to prevent human rights violations stemming from development and utilization of AI technologies, companies should proactively investigate their own impacts, included those occurring along their supply chains, through a process of human rights due diligence.[46] Corporate HRDD "consists in an on-going management process that a reasonable and prudent corporation has to undertake in order to meet its responsibility to respect human rights",[47] that

[42] In Europe, 'privacy by design' and 'privacy by default' are disciplined as core elements of the data protection legal regime by Art. 25 of the GDPR (Regulation 2016/679/EU 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*). According to this provision, controllers have to implement appropriate technical and organisational measures and necessary safeguards, designed to implement data protection principles in an effective manner and to protect the rights and freedoms of data subjects (see also European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, adopted on 13 November 2019, para 12 ff.). As to the literature, see: R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO G. RESTA, (a cura di), *Codice della privacy e data protection*, Giuffré, Milano 2021; A.E. WALDMAN, *Data Protection by Design? A Critique of Article 25 of the GDPR*, in Cornell International Law Journal, 2020, Vol. 53, No. 1, p. 147-167; L.A. BYGRAVE, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, in Oslo Law Review, 2017, pp. 105-120.

[43] See Art. 35 (3) a GDPR.

[44] As to human rights by design in AI, see: E. DONAHOE, M. METZGER, (2019), *Artificial Intelligence and Human Rights*, 2020, in Journal of Democracy, pp. 115-126; P. NEMITZ, *Constitutional Democracy and Technology in the Age of Artificial Intelligence*, in Phil. Trans. R. Soc. A, 2018, pp. 1-13; J. PENNEY, S. MCKUNE, L. GILL, R.J. DEIBERT, *Advancing Human-Rights-By-Design In The Dual-Use Technology Industry*, in Journal of International Affairs, 2018, pp. 103–110.

[45] See Principle 17 of the UNGPs.

[46] Of course, where business enterprises have large numbers of entities in their value chains it may be unreasonably difficult to conduct due diligence for adverse human rights impacts across them all. In this case, business enterprises should identify general areas where the risk of adverse human rights impacts is most significant, whether due to certain suppliers' or clients' operating context, the particular operations, products or services involved, or other relevant considerations, and prioritize these for human rights due diligence.

[47] See UN Human Rights Office of the High Commissioner, *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide*, 6 (2012).

has to be used to identify, prevent, mitigate and account for how they address their adverse human rights impacts.[48] It should include the following four core components: *a*) identifying and assessing actual or potential adverse human rights impacts; *b*) integrating and acting upon the findings; *c*) tracking responses; *d*) communicating how impacts are addressed. Corporate HRDD operates as a risk assessment tool and therefore can be included within broader enterprise risk management systems, provided that it goes beyond simply identifying and managing material risks to the company itself to include risks to rights-holders.[49] Exactly from this side, HRDD shares common grounds with the abovementioned 'privacy by design' approach.[50]

The relevance of such a process for companies developing or deploying AI technologies is self-evident. First, companies should identify, assess, and mitigate the actual and potential adverse human rights impacts of their *products* and *services*, not just sites, factories, farms, and corporate offices, and this in respect to their entire supply chain. This means that data-sets, algorithms, insights, intelligence, and alike applications should be subject to proactive human rights due diligence. Second, different actors across the value chain of a given product – such as suppliers, subcontractors, manufacturers, brands, licensees, franchises, retailers, traders, and customers – all have a responsibility to address adverse impacts. Yet, corporate HRDD shall apply to all companies irrespectively, of their dimension, size and the industrial sector of their business. HRDD processes, in sum, shall cover situations concerning the development and deployment of AI technologies where, for example, companies, must demonstrate that they have taken all the appropriate measures to ensure protection of human rights which may be potentially impaired by AI, algorithm, machine learning, etc.

In addition, and an extremely relevant point, a core element of a corporate HRDD practice resides in having in place policies and processes through which companies can 'know and show' that they respect

[48] As far as the nature of the corporate human rights due diligence under the UNGPs, which merges the due diligence notion as applied in corporate business practice with the same concept as applied within international human rights law, see M. FASCIGLIONE, *The Enforcement of Corporate Human Rights Due Diligence: From the UN Guiding Principles on Business and Human Rights to the Legal Systems of the EU Countries*, in Human Rights and International Legal Discourse, 2016, vol. 1, pp. 94-116. The 'amphibian' nature of corporate HRDD is also highlighted by J. BONNITCHA, R. MCCORQUODALE, *The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights*, in European Journal of International Law, 2017, vol. 28, pp. 899-919.

[49] Operatively, human rights due diligence should be initiated as early as possible in the development of a new activity or relationship, given that human rights risks can be increased or mitigated already at the stage of structuring contracts or other agreements, and may be inherited through mergers or acquisitions.

[50] Risk-based approach seems being at the heart of the proposal of the European Commission for a Regulation on AI (see European Commission, *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). The proposal aims to ensure that high-risk AI systems are designed and used in compliance with fundamental rights and that competent national authorities and courts can more effectively investigate and address possible breaches of fundamental rights obligations. Unfortunately, the proposal does not include any reference to the UNGPs, to corporate HRDD, neither to other international business and human rights standard fixing for companies due diligence and risk-based approach on human rights.

human rights in practice. 'Showing' involves communication to the public, and providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders, including investors. From this perspective, requesting hi-tech companies developing or deploying AI technologies to carry out due diligence in respect their impact on human rights, is a useful tool for helping them to increase the "explainability of their AI solutions"[51] and, accordingly, can prove to fill in a systemic gap in current regulation efforts on AI: *i.e.* the lack of sufficient information and transparency experienced by the wider public as to capabilities and impacts of AI.[52]

Despite their nature of soft law standards, nothing prevents corporate responsibility to respect and the corporate HRDD from inspiring multistakeholder and other kind of initiatives encompassing private sector, States and actors from the civil society, or even their "normative hardening" via domestic legislations.[53] Some interesting recent developments deserve to be mentioned in this respect.

UNGPs and the duty to perform human rights due diligence have clearly inspired the 2018 Toronto Declaration on Protecting the Right to Equality and Non-discrimination in Machine Learning Systems,[54] an NGOs-led declaration opened to the endorsement of State actors and private sector, urging States and private companies to take measures to promote respect for human rights, ensure accountability and provide effective remedies when creating or deploying AI technologies. Importantly, the Declaration invites private sector companies who "develop and deploy machine learning systems" to "follow a human rights due diligence framework". The Declaration calls on States and private companies to take measures to promote respect for human rights, ensure accountability and provide effective remedies when creating or deploying AI technologies. In addition, the Declaration requires hi-tech companies to disclose the process used to identify risks for human rights, the risks identified, and the concrete steps undertaken in order to prevent or mitigate them. This also implies the need to inform affected individuals about the harm and the means at their disposal for challenging it.[55]

Moreover, noteworthy normative developments occurred in several jurisdictions with the introduction of legislations either encouraging or mandating human rights due diligence and reporting. Under such

[51] See HRIC, HRIC Position Paper on Artificial Intelligence, 2020, p. 2.

[52] Algorithmic decision making is notoriously opaque: data collection, algorithm training, selection of data for modelling or profiling, the situation around individual consent, effectiveness and error rates of the algorithm, etc., are often not transparently reported. This represents a crucial challenge to the right to an effective remedy. See, FRA, *Getting the future right*, cit., FRA Opinion 6, p. 13, and p. 75 ff. In the literature, see P. NEMITZ, *Constitutional Democracy and Technology in the Age of Artificial Intelligence*, cit., p. 12; A.G. FERGUSON, *Policing Predictive Policing*, in Washington University Law Review, Vol. 94, 2017, pp. 1146-1150;

[53] C. BRIGHT, C. MACCHI, *Hardening Soft Law: The Implementation of Human Rights Due Diligence Requirements in Domestic Legislation*, M. BUSCEMI, N. LAZZERINI, L. MAGI, D. RUSSO (eds), in *Legal Sources in Business and Human Rights*, 2020, pp. 218–247.

[54] Amnesty International and Access Now, *The Toronto Declaration Protecting the right to equality and non-discrimination in machine learning systems*, 2018.

[55] See paras. 42 ff.

legislations companies may be addressees of specific duties concerning the protection of human rights negatively affected by business activities. Of course, these legislations may apply also to the development or utilization of AI technologies. As far as human rights reporting (mandatory disclosure) laws are concerned, not only an increasing number of national laws worldwide oblige companies to disclose information, mainly in respect to labour issues,[56] but also, and turning to the European regional level, human rights reporting has been established in specific EU secondary legislation.[57] In addition, legislations establishing overarching mandatory human rights due diligence deserve to be mentioned. Some of these legislations only apply to specific sectors such as conflict minerals, or child labour issues, while others have a larger scope and apply horizontally across human rights issues and across sectors. This is the case, as for instance, of the French Law on the Duty of Vigilance of Parent Companies adopted on 21 February 2017, and enacted on 27 March 2017[58] and of the German Supply Chain Due Diligence Act.[59] In the same vein, it should be stressed the vanguard role that EU is playing in respect to the crystallization of a harmonized European legal framework on mandatory corporate human rights due diligence. On 29 April 2020, the European Justice Commissioner, Didier Reynders, announced the commitment of the European Commission to the establishment of new rules on mandatory corporate human rights and environmental due diligence.[60] Among the large number of measures on which the future European legal instrument should rely,[61] the European Parliament has proposed that it should apply *a*) to all companies that are governed by the law of a Member State or established in the territory of the Union selling products or providing services into the internal market; *b*) to a company's own activities as well as those of its contractual counterparties and suppliers along the value chain; and *c*) in line with the UNGPs, to all internationally recognised human rights; *d*) all economic sectors, including the financial sector, shall be covered by this legal instrument. Preliminary provisions included in the

[56] See as for instance in the US the *California Transparency in Supply Chains Act* 2010 (US), s 1714.43(a)(1); or in the UK, *the Modern Slavery Act* adopted in 2015.

[57] See the EU Directive 2014/95 on Disclosure of Non-Financial Information (Parliament and Council Directive 2014/95/EU of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups.

[58] *Loi* No. 2017-399 du 27 mars 2017 *relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre*. As to the contents, the civil liability regime and the other enforcement measures fixed by the law, see S. BRABANT, E. SAVOUREY, *French Law on the Corporate Duty of Vigilance. A Practical and Multidimensional Perspective*, in Revue internationale de la compliance et de l'éthique des affaires – Dossier thématique, supplément à la semaine juridique entreprise et affaires, n° 50 du jeudi 14 décembre 2017.

[59] *Act on Corporate Due Diligence in Supply Chains*, adopted on 11 June 2021, in force since 2023.

[60] In March 2021 the European Parliament adopted the resolution with recommendations to the Commission on corporate due diligence and corporate accountability containing the proposal for a draft text of an European directive on corporate due diligence and corporate accountability (European Parliament, Corporate due diligence and corporate accountability European Parliament resolution of 10 March 2021 with recommendations to the Commission on corporate due diligence and corporate accountability, (2020/2129(INL), 10 March 2021).

[61] As to the legal form of the future secondary legislation to be adopted, the Draft Report proposes the form of a Directive.

European Parliament Briefings and Report represent, for hi-tech companies an important indicator of the likely elements of the new mandatory human rights due diligence regime and of the increasingly rigorous measures expected from the private sector in order to face the negative impacts on human rights, even in respect to AI and the cyberspace. By way of example, Art. 4 of the text recommended by the European Parliament establishes an obligation for EU companies to carry out effective due diligence with respect to potential or actual adverse impacts on human rights (as well as on the environment and good governance) in their operations and business relationships. According to the text recommended by the Parliament, companies shall not only carry out value chain due diligence, but shall have also *map* their value chain and publicly disclose relevant information about the undertaking's value chain, including names, locations, types of products and services supplied, and other relevant information concerning subsidiaries, suppliers and business partners in its value chain. The provision is clearly relevant to companies as they are requested to inform the public as to who are the (private and public) business partners of companies developing potentially human rights-impacting AI. Also, recent high profile legal cases,[62] civil society reports, and allegations brought to National Contact Points (NCPs) of the OECD Guidelines for Multinational Enterprises,[63] disclose that companies, spanning software designers, data collectors, telecommunications providers, cloud services, investors and venders, will be exposed by such mandatory legislations as well as the necessity that they be prepared for realizing human rights due diligence and to find ways to prevent, mitigate and redress the adverse human rights impacts of their operations worldwide.

6. Conclusions

The use of new technologies, such as AI, machine learning, facial recognition, is ever increasing. Policymakers have for some time highlighted the potential for AI and related technologies to improve efficiency and drive economic growth, with less emphasis on human rights impact. Only recently, due to the pressures coming from citizens, civil society and other vulnerable groups,[64] public authorities and

[62] In France, high executives of Amesys and Nexa Technologies, two hi-tech companies, have been charged with the crime of complicity in acts of torture for having sold surveillance equipment used to spy on political dissidents in Lybia and Egypt (see Business & Human Rights Resource Centre, *French executives of Amesys and Nexa Technologies face torture charges for selling spy gear to Libya, Egypt*, 22 June 2021)

[63] See NCP of Switzerland, *Initial Assessment Specific Instance regarding UBS Group AG submitted by the Society for Threatened Peoples Switzerlan*d, 20 January 2021, in which an NGO filed a specific instance to the Swiss NCP claiming possible human rights violations in the context of an alleged business relationship with the Chinese company Hangzhou Hikvision Digital Technology Co. Ltd. According to the submitting party, this company manufactured technology used for surveillance of the Uyghurs and other Turkic minorities living in the Xinjiang Uyghur Autonomous Region in China. By observing that a business relationship between UBS and Hikvision and a direct link between UBS's products and services and the alleged human rights violations could not be excluded with regard to the UBS financing operations, the Swiss NCP has admitted the specific instance for further considerations.

[64] See European Commission, 'Annex', in *Standard Eurobarometer*, n. 92, December 2019, p. T222 ff.

international organisations have started to scrutinize the fundamental rights challenges associated with such technologies. Coupled with the growing use and accuracy of AI systems, this has turned attention to whether and how to regulate their use and which actors should bear duties and responsibilities in this area. The growing reference to fundamental rights in debates and discussions indicates that a fundamental rights framework alongside other legal frameworks is necessary for an effective and human rights compliant evaluation of the many opportunities and challenges brought by new technologies. Even the most skeptical voices in this respect, nowadays acknowledge this necessity. AI human rights framework should be grounded on two principles of the utmost importance: the human-centric principle, and the accountability principle.[65] Both the principles point to ensuring that victims of human rights violations stemming from utilization of AI technologies have access to remedies.

As far as accountability is considered, it invites us to consider that it has to be assured that effective accountability systems are in place to monitor and, where needed, effectively address any negative impact of AI systems on fundamental rights. This principle suggests that today human rights violations often occur in a context characterized by joint and coordinated, rather than independent, actions from different duty-bearers, who through their conducts participate in various ways in assuring, or not, the protection of human rights. From this perspective the rise of the algorithmic society has only accelerated that already ongoing process, leading to "a paradigmatic change where the public power is no longer the only source of concern for the respect of fundamental rights and the protection of democracy".[66] It is thus precisely in such situation that integrating the State-individual matrix of human rights obligations with the corporate-individual matrix makes sense:[67] indeed, in the victim's eyes the nature of the violator, be it a public body or a private company, matters little. What is relevant for the victims, on the contrary, is that State legislation shall create conditions that are conducive to the respect for human rights by all AI actors and do not create barriers to effective accountability.

As far as human centrality is concerned, it refers of course to the necessity of ensuring effective oversight over potential human rights infringements stemming from intelligent systems, which implies that "the utilization of AI must not infringe upon the fundamental human rights guaranteed by the Constitution and international standards".[68] Human centrality also implies that AI systems must always remain under

[65] Both the principles have been widely advocated by international institutions and other regulatory bodies. See, among the others, FRA, *Getting the future right*, cit., pp. 8-10.

[66] See. O. POLLICINO, G. DE GREGORIO, *Constitutional Democracy in the Age of Algorithms: The Implications of Digital Private Powers on the Rule of Law in Times of Pandemics*, cit.

[67] For a recent analysis on how to conceptualize corporate accountability in current international legal system, especially with regard to the ongoing BHR treaty negotiation process, see N. BERNAZ, Conceptualizing Corporate Accountability in International Law: Models for a Business and Human Rights Treaty, in Human Rights Review, published online 17 October 2020.

[68] Government of Japan, *Social Principles of Human Centric AI*, March 2019.

human control, even in circumstances where machine learning or similar techniques allow for the AI system to make decisions independently of specific human intervention. In addition, human centrality also calls for a human rights-based approach that should guide hi-tech companies in developing and using AI. This approach requires that hi-tech companies conduct human rights due diligence, based on impact assessment and risk prevention in respect to any human rights violations they may cause, contribute or be linked to. States should establish a legal framework that sets out a procedure for public authorities and private companies, as well, to carry out human rights impact assessments (HRIAs): the UNGPs represent a largely acknowledged and accepted reference framework to look at in order to operationalize such an approach.

List of Contributors

- **Giorgia Bevilacqua,** *Researcher in International Law, Università della Campania Luigi Vanvitelli. Contact, giorgia.bevilacqua@unicampania.it*

- **Silvia Borelli,** *Director of Research, Principal Lecturer in Public International Law, University of Bedfordshire. Contact, silvia.borelli@beds.ac.uk*

- **Gianvito Brindisi,** *Associate Professor of Philosophy of Law, Università della Campania Luigi Vanvitelli. Contact, gianvito.brindisi@unicampania.it*

- **Roberta Catalano,** *Associate Professor of Private Law, Università della Campania Luigi Vanvitelli. Contact, roberta.catalano@unicampania.it*

- **Claudia Cinelli,** *Researcher in International Law, Università degli Studi di Pisa. Contact claudia.cinelli@unipi.it*

- **Adele Del Guercio,** *Researcher in International Law, University of Naples L'Orientale. Contact, adelguercio@unior.it*

- **Marco Fasciglione,** *Researcher in International Law, CNR-IRISS, Alternate member of the Management Board of the European Union Agency for Fundamental Rights (FRA). Contact, m.fasciglione@iriss.cnr.it*

- **Elena Gualco,** *Senior Lecturer in Law, University of Bedfordshire. Contact, elena.gualco@beds.ac.uk*

- **Ilaria Infante,** *PhD candidate in International Law, Università della Campania Luigi Vanvitelli. Contact, ilaria.infante@unicampania.it*

- **Kiara Neri,** *Maître de conférences (Associate Professor of International Law), Université Jean Moulin Lyon 3, Director of the International Law Center, Director of the Master Law of International Organisations. Contact, kiara.neri@univ-lyon3.fr*

- **Ana Nikodinovska Krstevska,** *Associate Professor of EU Law and EU Foreign policy, Goce Delcev University – Stip, Macedonia. Contact, ana.nikodinovska@ugd.edu.mk*

- **Maria Luisa Stasi,** *PhD candidate, Tilburg University, Tilburg Law School, Senior Associate ARTICLE 19. Contact, maria@article19.org*

- **Paolo Vignola,** *Professor of Esthetics and Literary Theory, Escuela de Literatura, Universidad de las Artes de Guayaquil, Ecuador; Technological University of Dublin. Contact, paolo.vignola@uartes.edu.ec*

- **Maria Chiara Vitucci,** *Full Professor of International Law, Università della Campania Luigi Vanvitelli. Contact, chiara.vitucci@unicampania.it*