Chapter 5
Open Issues and Conclusions

Contents

Abstract Having discussed in previous chapters the valuable contribution that an assessment model encompassing human rights, ethical and societal issues can provide to the development and regulation of AI, these concluding remarks address some of the challenges we face in implementing this approach in tangible reality. The focus on future global regulatory scenarios in the field of AI shows how the holistic HRESIA model, which includes the contextualisation of human rights and socio-ethical values in a given area, could be an effective answer for both the countries which have a human rights-based AI regulation and those who do not. In addition, holistic assessment and values-oriented design procedures can build trust in the development of AI, addressing the increasing public concern for invasive and pervasive AI applications, as well as the growing attention of policy makers to the side effects of AI use in the presence of concentration of power in digital services.

Keywords AI regulation · Data protection · Digital ecosystems · Human rights · Risk assessment · Trust

A. Mantelero, *Beyond Data*, Information Technology and Law Series 36,
https://doi.org/10.1007/978-94-6265-531-7_5

5.1 Addressing the Challenges of AI

For more than fifty years the progressive digitalisation and datafication of our societies and their impact on individuals have been largely managed by legislators through data protection laws. In a world concerned about the use (and misuse) of personal information, data protection became the key component in the response at individual and social level.

Since its origins, data protection has been seen as an enabling right to tackle potential risks concerning discrimination, undemocratic social control, invasion of private life, and limitations on several freedoms, such as freedom of thought, expression, and association.

However, this link between data protection and human rights (fundamental rights in the EU) has not been explored in the cases decided by the data protection authorities or in the literature.[1] Although the relationship between data protection and other competing rights has been considered in court decisions, the theory and practice of data protection remain largely remote from human rights doctrine and the attention of human rights experts. This also reflects the different backgrounds of the main scientific communities in these fields. Privacy scholars traditionally come from private, constitutional or administrative law, while human rights scholars have an international law background and are more focused on prejudice to human rights other than privacy and data protection.

This barrier between the two areas has collapsed under the blows of the latest wave of AI development, since the last decade of the twentieth century to the present day. Pervasive datafication together with the use of AI for a variety of activities impacting on society, from medicine to crime prevention, has raised serious concerns about the potentially harmful effects of data-intensive AI systems. This has led legislators and policymakers to look beyond data and data protection to consider the different ways in which AI might interfere with human organisations and behaviour, from automated decision-making process to behavioural targeting.

The breadth of the questions raised by AI and the relationship between machines (and those who determine their underlying values) and humans, the struggle of traditional data protection principles to fully address these new and broader issues,[2] and the limited discussion of human rights in AI led business and regulators to look to ethics for answers to these challenges.

However, the variety of ethical approaches stood in contrast to the need for a common framework in a world of global players and the same models replicated in different countries. This has led AI regulators to the current debate on a future legal framework, where human rights represent a key component in addressing the potential risks of AI.

Having briefly summarised the trajectory and after highlighting the valuable contribution that an assessment model encompassing human rights, ethical and

[1] Mantelero and Esposito 2021, para 4.

[2] See Chap. 1.

societal issues can provide, the big challenge that still faces us is how to implement this approach in tangible reality. Two different scenarios have to be taken into account: (i) AI development and use in countries where human rights are protected by national law and where compliance is therefore mandatory on business and the public sector, and (ii) AI development and use, by companies and their subsidiaries and suppliers, in countries where those rights are not fully protected, or not protected at all, despite the ratification of international human rights treaties. In any case, it has to be remembered that, in both cases, ethical and social issues remain largely outside the legal discourse and an awareness of AI's impact in these spheres remains lacking.

While in the first scenario HRESIA can be more easily implemented, where business is conducted in the absence of national human rights safeguards, the United Nations' Guiding Principles on Business and Human Rights may be of help.[3] These Principles, and specifically Section II on corporate responsibility to respect human rights, enshrine several key HRIA requirements (stakeholder consultation, regular assessment, transparency, role of experts, etc.).[4] While this is not a legally binding instrument, it does represent an influential global model in addressing the relationship between human rights and business.[5]

However, despite the presence of this authoritative framework, the impact of these principles is still limited, perhaps because of their focus on the entire value chain, which normally demands an extensive effort in all directions.[6] The ongoing debate on the Guiding Principles on Business and Human Rights and the challenges their application raises may point the way to narrower product-focused human rights assessments, such as the HRESIA, which spotlights the design of each product or service, rather than targeting the entire business.[7]

If the lack of legal safeguards for human rights at a national level is problematic, the situation is much more complicated when we consider the ethical and societal values underpinning AI development and use. Here, even proposed human rights-oriented regulations do not specifically address the societal acceptability of AI, and its compatibility with societal values is not fully reflected in the law.[8]

[3] See also United Nations High Commissioner for Human Rights 2021.

[4] United Nations 2011; Council of Europe, Committee of Ministers 2016. On the distinction between the approach adopted in UN Guiding Principles and Corporate Social Responsibility (CSR), and on the limitations of the latter, see Wettstein 2020.

[5] See also European Commission 2020, pp. 48–49. But see Deva 2013, who also points out the limits of transplanting international human rights instruments designed for state in a corporate business context.

[6] European Commission 2020, p. 41. But see United Nations 2011, Commentary to Principle 17, on product/service due diligence for adverse impacts on human rights where companies have a large number of entities in their value chains making it difficult to conduct an impacts assessment of all of them.

[7] For a broader approach, see Sect. 5.3.

[8] See Chap. 3.

Rather than try to arrive at improbable universal ethical and social values or, on the contrary, shape codes of ethics to fit corporate values, the best solution is probably to use experts to understand the context. Experts can help identify underlying societal values and also make for greater accuracy and inclusion through active dialogue with shareholders and participation.[9]

5.2 The Global Dimension of AI

As in the case of data processing, the global use of AI technologies is making regulation a pressing challenge. Although only a few proposals for AI regulation are available and as yet in their early stages, we can envisage what might happen in the future in terms of global regulatory competition and fragmentation.

On the one hand, Europe might build on its front runner status in data protection, to reproduce for AI the so-called Brussels effect,[10] as well as the Strasbourg effect,[11] exporting its regulatory model and risk-based approach including attention to human/fundamental rights.

On the other, it is worth recalling the limits of the universal human rights position[12] and European legislators' dependence on the European Court of Human Rights and the European Court of Justice, making it hard to export the European models to different legal contexts.[13]

In addition, regulatory fragmentation at a regional level may ensue from state policies targeting digital sovereignty, either with the intention to bolster human rights or on the contrary in countries wishing to limit these individual rights and freedoms.

This scenario is not new and was seen already with respect to data protection. Data localisation obligations and restrictions on transborder data flows were introduced by European countries under Convention 108 or the GDPR to provide their citizens with a greater level of protection than third countries with weaker data protection regimes, or to safeguard competing interests (national security, defence, public safety, etc.).[14] Meanwhile, some countries have introduced rules on transborder data flows and data localisation for foreign service providers, not to safeguard human rights, but as a means to secure governmental control over their citizens' online behaviour.

[9] See Chap. 3.

[10] Bradford 2020.

[11] Bygrave 2021.

[12] See Chap. 3, Sect. 3.1.1.

[13] Pauletto 2021.

[14] Convention 108+, Article 14, and GDPR, Chapter IV.

Replicating European progress in data protection[15] in the regulation of AI around the world therefore looks unlikely. Despite the worldwide interest in the EU and Council of Europe AI initiatives, we must remember that Convention 108 dates back to 1981 and the GDPR was built on a 1995 Directive. While we might envisage a Brussels/Strasbourg effect for AI, even conceding a faster international harmonisation in response to the globalisation of services, needs and trends, it is unrealistic to expect a common legal framework on AI to be realised any time soon. This is partly due to the difficulties of exporting the European models noted above, but also to the varying regulatory approaches of some states, in particular with respect to recognising human rights.

This means that at present a holistic assessment model, which includes the contextualisation of human rights and socio-ethical values in a given area, could be an effective answer for both the countries which have human rights-based AI regulation and those who do not. For the former, the HRESIA could be integrated into proposed AI risk assessment procedures,[16] while in the latter it would help companies and other bodies develop a new approach, recognising the impact of AI applications on society in line with human rights-oriented business practices.

Indeed, assessment models like the HRESIA do not need to be mandatory but could be voluntarily included in business and public sector best practices when dealing with legal and societal needs. Of course, the mandatory or voluntary obligation to carry out the assessment would impact its adoption and the achievement of its goals.

The absence of a mandatory obligation would only reinforce concerns already expressed about the self-assessment of AI risks,[17] pointing to the conflicting interests of AI manufacturers and users. Further, while the danger of unfair risk assessment exists, both the mandatory and voluntary schemes are open to manipulation, and internal mitigation measures could be taken to combat this.[18]

Moreover, the new notion of trustworthy AI, though based on a non-legal and uncertain frame of reference (trust), highlights the importance of the relationship between AI providers/users and end-users. A wider adoption of impact assessments by providers/users can certainly play a part in boosting confidence among AI end-users.

Given the increasing public concern for invasive and pervasive data-intensive applications,[19] plus the growing attention of policy makers for the side effects of their use in the presence of concentration of power in digital services, building trust has become a major goal for AI providers and users. Though a variety of strategies (including marketing) can be used to achieve this, implementation of a risk

[15] Greenleaf 2021.

[16] See Chap. 4.

[17] E.g., AlgorithmWatch 2021, p. 5.

[18] The HRESIA model includes several features to reduce this risk, see Chap. 2.

[19] E.g., Veliz 2021; Zuboff 2020; O’Neil 2017.

assessment model with its transparent outcomes and practices can be an effective way to develop genuinely trustworthy AI.

Adopting holistic assessment and values-oriented design procedures such as the HRESIA could therefore replicate in AI the experience and results achieved in other sectors with regard to human rights and ethical practice, including the repercussions for business reputation[20] and consumer/investor choices[21] (e.g. fair trade labels).[22] The implementation might even be certified. Here, the effect on the biggest AI adopters (e.g. municipalities) would be even more significant if they were accountable to AI end-users.

Besides, a greater focus on these requirements by the big players and in public procurement[23] could also help override the scarce interest in these issues of many AI start-ups and SMEs. A bottom-up demand for responsible AI, supported by appropriate assessment models, could counter the lack of focus on societal and human rights questions due to an absence of competence or attention to aspects that are not immediately related to business profits.[24]

On the other hand, following the European model in introducing a mandatory AI human rights impact assessment[25]– hopefully extended to non-legal societal issues – would undoubtedly foster a quicker diffusion of this practice.[26] But this option has its own implications that need to be thought through.

In the first place, a universal mandatory assessment might provoke adverse reactions from businesses complaining of additional burdens and costs. While these are proportional to the complexity of the AI and risks in question, legislators could be induced (see the EU proposal) to restrict mandatory assessments to certain categories of applications. This could result in a dual situation, with some areas fully secured and monitored (or even over-scrutinised, given the broad categories in the AIA proposal, potentially including non high-risk applications) while other widespread AI uses go largely unregulated despite their not insignificant risks.

Second, the history of data protection reveals the difference between the ambitions of the law and its concrete implementation. Underfunded and understaffed supervisory authorities, pervasive adoption of data-intensive solutions, obscurity of processing operations, foreign providers, interplay between AI developers and

[20] See also Spiekermann 2016, pp. 184–85.

[21] European Commission 2020, pp. 89–90.

[22] E.g., Castaldo et al. 2009; Bartels et al. 2020.

[23] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) 2019, para 3.2. See also Wylie 2020; United Nations 2011, p. 6.

[24] Powell 2021.

[25] See also European Parliament 2021.

[26] Wagner 2018, who highlights that, in the field of Corporate Social Responsibility, the development of non-financial reporting practices "is an evolutionary process that may take years to accomplish as countries adapt to new and changing circumstances pertaining to such reporting", even when supported by specific law provisions.

governments, are all factors that may reduce the enforcement of mandatory solutions, as happened with data protection.[27]

Very likely in coming years both mandatory and non-mandatory AI risk assessment models will coexist and may include the adoption of technical standards. A middle way based on ex post assessment is also possible, in response to concerns by some supervisory authorities. Here the dual dimension of the HRESIA model, in its universal and local treatment of human rights and societal values, might also make it a useful tool for supervisory authorities.

Finally, the global scenario in which AI should be seen also highlights the value of a risk-based approach from the perspective of the historical development of system use. Particularly in the public sector, the lack of attention to human rights and societal impact can encourage a sort of development bias, which sees only the positive results of AI and disregards or underestimates potential misuse. As recently demonstrated by the use of data-intensive biometric systems in Afghanistan[28] (as well as some contact-tracing applications during the Covid-19 pandemic[29]), the lack of a holistic assessment of the potential consequences of AI-based systems can be damaging. It also fails to give voice to minorities, affected groups and stakeholders, leading to technology-driven solutions whose efficiency is not accompanied by an absence of risks when operating conditions or the system controllers change.

5.3 Future Scenarios

A thread running through this book has been the idea of looking beyond data protection to tackle the challenges of AI and avoid a split between the focus on human rights and ethics in the broader sense. While today a growing number of voices are calling for a human rights assessment, this option was largely unexplored at the start of this research, and the question of how to put a human rights-based approach to AI into practice remains little examined.

The first chapter pointed out the reason for this change of focus in the regulation of AI data-intensive systems from data protection to human rights and highlighted the role that assessment methodologies can play in this change.

A workable methodology that responds to the new paradigm can also help to bridge the gap between the ethical guidelines and practices developed in the last few years and the more recent hard law approach. Here the regulatory turn missed an opportunity to combine these two realms, both of which are significant when AI applications are used in a social context and have an impact on individuals and groups.

[27] See also Schilling-Vacaflor 2021.

[28] Privacy International 2021.

[29] United Nations et al. 2020; Council of Europe 2020.

Shaping AI on the basis a paradigm that rests on legal and societal values through risk assessment procedures does not mean simply crafting a questionnaire with separate blocks of questions for legal issues, ethical values and social impact. Such a simplistic approach tends to overestimate the value of the questionnaire-based self-assessment[30] and ignores the challenges associated with the idea that AI developers/users can fully perform this evaluation as if it were a mere checklist.

Chapters 2 and 3 therefore outline a more elaborate model, the HRESIA (Human Rights, Ethical and Social Impact Assessment), which combines different tools ranging from self-assessment, expert panels, to participation. The biggest distinction to be made here is between the Human Rights Impact Assessment (HRIA) module of the HRESIA and the complete evaluation of ethical and societal values. While the first is based on questionnaires and risk models, the second is characterised by a greater role for experts and participation in identifying the values to be embedded in AI solutions. Furthermore, the HRIA component, though based on lengthy experience in human rights assessment, has reshaped the traditional model to make it better suited to AI applications and an increasingly popular regulatory approach based on risk thresholds and prior assessment.

This interplay between risk assessment and AI regulation led to an examination of the major current proposals, presented by the European Commission and the Council of Europe. Chapter 4 emphasised their limitations compared with the HRESIA model, by not including ethical and social issues and (in the EU case) restricting risk assessment to predefined high-risk categories. It should be noted however that the Council of Europe's proposal does broaden the assessment to include democracy and the rule of law, in line with its mandate, but at the same time making it more complicated to envisage a feasible assessment model that properly covers all these issues without reducing them to a mere list of questions.

As regards the social and ethical components in the design and operation of AI systems and assessing their coherence with contextual values, Chap. 3 explored the practices of ethics committees considering both committees set up by companies and committees in the field of medical ethics and research. Their experience, and their shortcomings, were used to highlight the role of experts in the HRESIA in identifying key societal values and also to outline how these committees might work, including with the participation of major stakeholders and groups potentially affected by AI applications.

Comparison of the HRESIA with its various components and the ongoing proposals for AI regulation show how the HRESIA can represent a better implementation of the risk-based approach adopted by European legislators and, in a global perspective, encourage a focus on the holistic consequences for society in countries where there are no regulations.

Notwithstanding the positive outcomes that a better understanding of human rights and societal values can bring to AI design, development and use, the longer

[30] Sarfaty 2013.

term poses further questions that are not fully addressed by the HRESIA and it may be that we have to raise the bar of human rights expectations with respect to an AI-based society. Three main issues will dominate discussion and analysis over the coming years: (i) partial reconsideration of the traditional theoretical framework of human rights; (ii) extension of the requirements concerning human rights safeguards, but also compliance with ethical and social values, to the entire AI supply chain; (iii) a broader reflection on digital ecosystems.

As for the first issue, there is an ongoing debate on the collective dimension of human rights which is leading us to reconsider the traditional view taken in this field.[31] The classification of the world by AI and its consequent decision-making processes, irrespective of the identity of the targeted persons and based merely on their belonging to a certain group, suggests we need a broader discussion of the largely individual nature of human rights.

Similarly, the traditional approach to non-discrimination should be reconsidered. Here intersectional studies and other theories can contribute to providing a legal framework more responsive to the new AI scenario.[32] Nevertheless, the variety of criteria used by business to discriminate in AI and their lack of a link to protected grounds suggests more research called for into the blurred confines between unfair discrimination and unfair commercial practices.[33]

Moving from the theoretical framework to impact assessment implementation, this book has focused on the impact of AI-based solutions on their potential social targets, looking forward to the effects of AI use. But we need to extend the same attention to the upstream stage of this process, namely compliance with human rights and ethical values, as well as the social acceptability of manufacturing practices and the AI products/services supply chain.[34]

[31] Newman 2004; Mitnick 2018, p. 6; Hartney 1991.

[32] Mann and Matzner 2019; Hoffmann 2019. See also Wachter et al. 2021.

[33] Ebers 2021; Galli 2020.

[34] European Commission 2020, p. 16 (“Just over one-third of business respondents indicated that their companies undertake due diligence which takes into account all human rights and environmental impacts, and a further one-third undertake due diligence limited to certain areas. However, the majority of business respondents which are undertaking due diligence include first tier suppliers only. Due diligence practices beyond the first tier and for the downstream value chain were significantly lower. The vast majority of business stakeholders cover environmental impacts, including climate change, in their due diligence, although the term ‘climate change due diligence’ for a self-standing process is currently rarely used, and human rights and climate change processes often take place in ‘silos’. The most frequently used due diligence actions include contractual clauses, codes of conduct and audits.”).

New studies are emerging in this field,[35] but it remains largely unexplored, especially with regard to the possible solutions in terms of policies and regulation. Aspects such as labour exploitation or the environment impact of AI solutions need to be examined not only for the benefit of AI adoption and development, but also of competition. Existing and proposed barriers to market entry are based on legal requirements and standards on product safety and the human rights impact of AI use, but ignore human rights violations in the production of AI.

While some personal data protection is possible when data subjects belong to countries with robust data protection regulations,[36] in other cases rights and freedoms are more difficult to protect. This is particularly true when the legal systems of AI producer countries lack effective human rights protection or enforcement. The UN Guiding Principles on Business and Human Rights can serve as a guide in these cases.

Barriers to market access,[37] but also mandatory obligations on human rights and fundamental freedoms as well as due diligence[38] for subcontractors can be an important step forward in extending human rights to upstream AI manufacturing, in part following the experience of data protection, but also the EU's ethical rules on biomedicine and research. This would contribute to an improved AI ecosystem where respect for human rights and ethical and social values are widely accepted as a condition for doing business, in the same way ethical and legal compliance is a requirement of the pharma industry.

Reference to the AI ecosystem brings us to a final forward-looking scenario regarding the ability to outline an ecology for the digital environment, including AI-based applications which will increasingly become its dominant components.

Despite the limited investigation of this topic, we urgently need to revise the approach to digital technology adopted in the wake of the computer revolution in the 1950s. The increasing availability of new, more powerful and cheaper solutions led to the pervasive presence of digital technologies with their limitless appetite for data and the escalating reliance on them by decision makers. The result is a world that is seen more and more through the lens of algorithms and the social values and

[35] Crawford 2021. See also Crawford and Joler 2018.

[36] E.g., European Data Protection Board (2021). Swedish DPA: Police unlawfully used facial recognition app https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en. Accessed 28 March 2021. The decision of the Swedish SA is available (in Swedish) at https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-polismyndigheten-cvai.pdf. Accessed 28 March 2021.

[37] See also European Parliament 2021, n. 10.

[38] United Nations 2011, p. 15, on the notion of due diligence, ("A human rights due diligence process to identify, prevent, mitigate and account for how they [rights, business enterprises] address their impacts on human rights"). This position is also reflected in the ILO Tripartite declaration of principles concerning multinational enterprises and social policy (MNE Declaration) revised in 2017, and in the UN Global Compact. But see the critical observations, about the use of this notion in the human rights context, made by Deva 2013, pp. 98–101.

standpoints of their developers, often without questioning the real need for such systems.[39]

Just as industrial consumer societies are raising questions about the ecological sustainability of the apparently endless abundance of goods and services, the digital society must also question the need for, and acceptability of, a society increasingly governed by pervasive AI. This includes critical questions about the lack of democratic participation and oversight in shaping and adopting AI solutions.

The starting point should not be to see technological evolution as an inevitability that society must adapt to, but to question the desirability of a society based on microtargeting, profiling, social mapping, etc. where the trade-offs for democracy, human rights and freedoms are not necessarily positive, except in the rhetoric of service providers and decision makers who place cost reductions and efficiency at the top of their scale of values.

References

AlgorithmWatch (2021) Draft AI Act: EU Needs to Live up to Its Own Ambitions in Terms of Governance and Enforcement. https://algorithmwatch.org/en/wp-content/uploads/2021/08/EU-AI-Act-Consultation-Submission-by-AlgorithmWatch-August-2021.pdf. Accessed 6 August 2021.

Bartels J, Reinders MJ, Broersen C, Hendriks S (2020) Communicating the Fair Trade Message: The Roles of Reputation and Fit. International Journal of Advertising 39(4): 523–547.

Bradford A (2020) Brussels Effect: how the European Union rules the world. Oxford University Press, New York.

Bygrave LA (2021) The ‘Strasbourg Effect’ on data protection in light of the ‘Brussels Effect’: Logic, mechanics and prospects. Computer Law & Security Review 40, https://doi.org/10.1016/j.clsr.2020.105460.

Castaldo S, Perrini F, Misani N, Tencati A (2009) The missing link between corporate social responsibility and consumer trust: The case of fair trade products. Journal of Business Ethics 84:1–15.

Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) (2019) Guidelines on Artificial Intelligence and data protection, T-PD(2019)01. https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8. Accessed 15 April 2020.

Council of Europe (2020) Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7 Accessed 8 May 2020.

Council of Europe, Committee of Ministers (2016) Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business.

Crawford K (2021) Atlas of AI : Power, Politics, and the Planetary Costs of Artificial Intelligence : Power, Politics, and the Planetary Costs of Artificial Intelligence. Yale University Press, New Haven.

[39] See the Sidewalk Toronto case in Chap. 2.

Crawford K, Joler V (2018) Anatomy of an AI System: The Amazon Echo As An Anatomical Map of Human Labor, Data and Planetary Resources. AI Now Institute and Share Lab. http://www.anatomyof.ai. Accessed 27 December 2019.

Deva S (2013) Treating Human Rights Lightly: A Critique of the Consensus Rhetoric and the Language Employed by the Guiding Principles. In: Bilchitz D, Deva S (eds) Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect? Cambridge University Press, Cambridge, pp 78–104.

Ebers M (2021) Liability for Artificial Intelligence and EU Consumer Law. JIPITEC 12:204-220.

European Commission (2020) Study on Due Diligence Requirements through the Supply Chain: Final Report. https://doi.org/10.2838/39830. Accessed 11 July 2021.

European Parliament (2021) Report with Recommendations to the Commission on Corporate Due Diligence and Corporate Accountability. https://www.europarl.europa.eu/doceo/document/A-9-2021-0018_EN.pdf. Accessed 11 July 2021.

Galli F (2020) Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD. In: Ebers M, Cantero Gamito M (eds) Algorithmic Governance and Governance of Algorithms. Springer, Cham, pp 109–135.

Greenleaf G (2021) Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance 169 Privacy Laws & Business International Report 1. https://papers.ssrn.com/abstract=3836348. Accessed 30 September 2021.

Hartney M (1991) Some Confusions Concerning Collective Rights. Canadian Journal of Law & Jurisprudence 4(2):293–314.

Hoffmann AL (2019) Where Fairness Fails: Data, Algorithms, and the Limits of Antidiscrimination Discourse. Information, Communication & Society 22(7):900–915.

Mann M, Matzner T (2019) Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination. Big Data & Society 6, https://doi.org/10.1177/2053951719895805.

Mantelero A, Esposito MS (2021) An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems. Computer Law & Sec. Rev. 41 https://doi.org/10.1016/j.clsr.2021.105561.

Mitnick EJ (2018) Rights, Groups, and Self-Invention : Group-Differentiated Rights in Liberal Theory. Routledge, New York.

Newman DG (2004) Collective Interests and Collective Rights. American Journal of Jurisprudence 49(1):127–163.

O'Neil C (2017) Weapons of math destruction : how big data increases inequality and threatens democracy. Broadway Books, New York.

Pauletto C (2021) Options towards a global standard for the protection of individuals with regard to the processing of personal data. Computer Law & Sec. Rev. 40, https://doi.org/10.1016/j.clsr.2020.105433.

Powell AB (2021) Undoing optimization: civic action in smart cities. Yale University Press, New Haven.

Privacy International (2021) Afghanistan: What Now After Two Decades of Building Data-Intensive Systems? http://privacyinternational.org/news-analysis/4615/afghanistan-what-now-after-two-decades-building-data-intensive-systems. Accessed 30 September 2021.

Sarfaty GA (2013) Regulating Through Numbers: A Case Study of Corporate Sustainability Reporting. Va J Int'l L 53(3):575–621.

Schilling-Vacaflor A (2021) Putting the French Duty of Vigilance Law in Context: Towards Corporate Accountability for Human Rights Violations in the Global South? Human Rights Review 22:109–127.

Spiekermann S (2016) Ethical IT innovation : a value-based system design approach. CRC Press, Boca Raton.

United Nations (2011) Guiding Principles on Business and Human Rights. https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. Accessed 8 December 2020.

United Nations, IOM, ITU, OCHA, OHCHR, UNDP, UNEP, UNESCO, UNHCR, UNICEF, UNOPS, UPU, UN Volunteers, UN Women, WFP, WHO (2020) Joint Statement on Data

Protection and Privacy in the COVID-19 Response. https://www.who.int/news/item/19-11-2020-joint-statement-on-data-protection-and-privacy-in-the-covid-19-response. Accessed 26 November 2020.

United Nations High Commissioner for Human Rights (2021) The Right to Privacy in the Digital Age. Report of the United Nations High Commissioner for Human Rights. https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx. Accessed 15 September 2021.

Veliz C (2021) Privacy is Power. Why and How You Should Take Back Control of Your Data. Corgi Books, London.

Wachter S, Mittelstadt B, Russell C (2021) Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI. Computer Law & Security Review 41, https://doi.org/10.1016/j.clsr.2021.105567.

Wagner CZ (2018) Evolving Norms of Corporate Social Responsibility: Lessons Learned from the European Union Directive On Non-Financial Reporting. Transactions: The Tennessee Journal of Business Law 19:619–708.

Wettstein F (2020) The History of Business and Human Rights and Its Relationship with Corporate Social Responsibility. In: Deva S, Birchall D (eds) Research Handbook on Human Rights and Business. Edward Elgar Publishing, Cheltenham/Northampton, MA, pp 23–45.

Wylie B (2020) In Toronto, Google's Attempt to Privatize Government Fails—For Now. Boston Review. https://bostonreview.net/politics/bianca-wylie-no-google-yes-democracy-toronto. Accessed 2 June 2020.

Zuboff S (2020) The age of surveillance capitalism: the fight for a human future at the new frontier of power. PublicAffairs, New York.