Regulating Digital and AI Technologies:

Lessons from the Digitisation of Contact Tracing during the COVID-19 Pandemic

*Lorna McGregor**

1 Introduction**

International human rights law, international disaster law, and the International Health Regulations all require states to act with due diligence to prevent, mitigate, and remedy specific harms generated by global health pandemics, including grave threats to life and health.[1] However, each body of law only provides partial direction on the nature of the measures states are expected to adopt. In common with the wider shift within the public sector to "digital", "algorithmic" or "AI" government,[2] the question arises whether digital technologies form part of the measures expected – or even required of – states in a global health pandemic.

No common definition of digital technologies exists but technologies often arranged under this heading include smart technologies, the Internet of Things, blockchain, and artificial intelligence (AI) technologies.[3] 'AI' similarly does not denote a particular technology but also acts as an umbrella term to group a range of new and emerging technologies.[4] The draft EU Artificial Intelligence Act defines an AI system as 'software that is developed with one or more of the techniques and approaches listed in Annex I [such as 'machine learning approaches'; 'logic and knowledge-based approaches'; '[s]tatistical

* Professor of International Human Rights Law and PI, ESRC Human Rights, Big Data and Technology Project, University of Essex.

** This work was supported by the Economic and Social Research Council [grant number ES/M010236/1]. The author would like to thank Alexandra Ziaka for her extensive research support for this article.

1 Antonio Coco and Talita de Souza Dias, 'Prevent, Respond, Cooperate: States' Due Diligence Duties vis-à-vis the Covid-19 Pandemic', (2020) 11 Journal of International Humanitarian Legal Studies.

2 *Ibid.*

3 See, Zeynep Engin and Philip Treleaven, 'Algorithmic Government: Automating Public Services and Supporting Civil Servants in Using Data Science Technologies', (2019) 62 Computer Law Journal, 457.

4 Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, 'A Definition of AI: Main Capabilities and Disciplines' (8 April 2019).

approaches, Bayesian estimation, search and optimization methods'] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environment they interact with'.[5] While this definition focuses on the task of specific AI technologies, they often form part of a wider system. For example, when defining AI, the Office for Artificial Intelligence in the UK's Government Digital Services provides examples of the contribution of AI to systems such as self-driving cars and speech recognition.[6] As discussed in this article, these illustrations indicate that defining or classifying AI technologies – particularly in assessing whether states are expected or required to employ them as part of preparation or response to global health pandemics – may not be as straightforward as focusing on specific technological 'techniques and approaches'. It may also require a wider lens that encompasses the overall system in which they function, including the data which feeds, and is produced, by such technologies.

Early in the COVID-19 pandemic, the World Health Organization and other actors anticipated that digital technologies, including AI, would play a central role in dealing with the pandemic. These technologies ranged from the delivery of remote education and work through digital platforms; to access to healthcare online; to the use of AI technologies to model, analyse, and predict the spread of the virus, thereby informing states on their selection of measures to protect the rights to life and the highest attainable standard of health ('right to health').[7] Reviewing literature on AI technologies during the pandemic, Ilana Harrus and Jessica Wyndham summarise five application areas as '1) applications applied to forecast the spread of the virus, 2) medical applications to diagnose the disease, 3) applications to contain and monitor the spread of the disease, 4) applications to develop drugs and treatments, and 5) applications for social and medical management including workforce relief and supply chain optimization'.[8]

In this regard, digital technologies, particularly when AI-enabled, may bring new and unique insights which may advance human rights, including

5 Article 3(1).

6 Office of Artificial Intelligence of the UK Government Digital Service, 'A Guide to Using Artificial Intelligence in the Public Sector' (2020) 6.

7 'Artificial Intelligence and Covid-19', The British Medical Journal (collection of articles proposed and funded by the World Health Organization), available at <https://www.bmj.com/AIcovid19>, last accessed (as any subsequent URL) on 15 August 2021. See also, Yann Sweeney, 'Tracking the debate on COVID-19 surveillance tools', (2020) 2 Nature Machine Intelligence, 323 (noting the potential role of AI in modelling).

8 Ilana Harrus and Jessica Wyndham, 'Artificial Intelligence and COVID-19: Applications and impact assessment', American Association for the Advancement of Science (March 2021).

the rights to life and health during a pandemic. However, as is now well-documented, even when designed or deployed to address global challenges or meet due diligence obligations, digital technologies can present serious risks, including to human rights. These risks may arise from: the design and functioning of a particular type or model of technology; the involvement of particular actors, including private companies; the context and purpose(s) of use; and the nature of the governance models in place. These risks may be accentuated where AI is involved, by enabling widescale surveillance, behavioural profiling, and the use of predictive analytics, including to make major decisions on our lives.[9] These factors influence whether risks materialise as well as their nature and scale.

To date, no comprehensive or dedicated international regulation exists to guide states' decisions on whether and how to employ digital technologies, including AI, within a global health pandemic or in other contexts. However, as noted above, the EU Artificial Intelligence Act is in draft form;[10] the UN Human Rights Council has issued relevant resolutions including two on the right to privacy in the digital age;[11] some states have produced national AI strategies;[12] and many actors have advanced soft law standards on ethical and

9 Access Now, 'Human Rights in the Age of Artificial Intelligence' (2019); Lorna McGregor, Daragh Murray, Vivian Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability' (2019) 68/2 International and Comparative Law Quarterly, 309; Lorna McGregor, Vivian Ng and Ahmed Shaheed, 'Universal Declaration of Human Rights at 70: Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence' (2019); Sarah West, Meredith Whittaker, and Kate Crawford, 'Discriminating Systems: Gender, Race and Power in AI', AI Now Institute (April 2019) available at <https://ainowinstitute.org/discriminatingsystems.html>. For discussions on risks arising in the public sector, specifically, see, Bernd Wirtz, Jan Weyerer and Carolin Geyer, 'Artificial Intelligence and the Public Sector', (2019) 42 International Journal of Public Administration, 596; Ryan Calo and Danielle Keats Citron, 'The Automated Administrative State: A Crisis of Legitimacy', (2021) 70 Emory Law Journal, 797; Kate Crawford and Jason Schulz, 'AI Systems as State Actors', (2019) 119 Columbia Law Review, 1941.

10 However, 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', Brussels, 21.4.2021 COM(2021) 206 final.

11 UN General Assembly, 'Resolution Adopted by the Human Rights Council on 23 March 2017' A/HRC/RES/34/7 (7 April 2017); UN General Assembly, 'The Right to Privacy in the Digital Age' A/HRC/42/L.18 (24 September 2019).

12 See, for example, Anna Jobin, Marcello Ienca, and Effy Vayena, 'The Global Landscape of AI Ethics Guidelines' (2019) Nature Machine Intelligence; Vincent Van Roy, Fiammetta Rossetti, Karine Perset and Laura Galindo-Romero, 'AI Watch – National strategies on

human rights-based approaches to AI.[13] Moreover, these technologies do not exist in a regulatory void. Data protection legislation, such as the EU General Data Protection Regulation, provides partial coverage of the use of digital technologies, where their use entails data processing. While not technology-specific, existing laws, such as public[14] and human rights law,[15] also apply to the use of digital technologies. This includes the 1984 Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (Siracusa Principles) which provide a framework for states to approach derogations and limitations to human rights, including when adopting public health measures to deal with pandemics, again even if not technology-specific.

Using the example of the digitisation of contact tracing during the COVID-19 pandemic, I discuss the challenges that arise from seeking to use digital technologies, particularly where they involve AI dimensions, as part of states' due diligence obligations while addressing risk in the absence of any, or incomplete, regulation dedicated to the governance of these technologies. As quickly became apparent, contact tracing via an app is a qualitatively different exercise to simply digitising a human function.

While many articles refer to contact tracing apps as 'AI-enabled',[16] in practice the classification of contact tracing apps as simply 'digital' (for example, through the use of Bluetooth technologies to enable smartphones in close proximity to send signals to each other indicating potential exposure[17]) or 'AI',

---

Artificial Intelligence: A European perspective', 2021 edition, Publications Office of the European Union (2021).

13 The organisation Algorithm Watch maintains the 'AI Ethics Guidelines Global Inventory' that 'maps frameworks that seek to set out principles of how systems for automated decision-making' and currently contains 173 guidelines (last checked 22 August 2021), available at <https://inventory.algorithmwatch.org>; see also, Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy and Madhulika Srikumar, 'Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI', Berkman Klein Research Publication No. 2020–1 (15 January 2020).

14 Jennifer Cobbe, 'Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making', (2019) 39 Legal Studies.

15 See McGregor, Murray and Ng (n 9).

16 See, for example, Ramzi El-Haddadeh, Adam Fadlalla and Nitham M. Hindi, 'Is There a Place for Responsible Artificial Intelligence in Pandemics? A Tale of Two Countries', Information Systems Frontiers (2021).

17 Leesa Lin and Zhiyuan Hou, 'Combat COVID-19 with artificial intelligence and big data', (2020) Journal of Travel Medicine, 3.

depends on their design, operating system and governance.[18] In this regard, some contact tracing apps form part of a wider contact tracing system which stores data from the apps (in identifiable or anonymised form) centrally and analyses it using machine learning technologies to facilitate contact tracing.[19] In some instances, the data is combined with other data sources held by the state and businesses and analysed through machine learning techniques.[20] The more 'AI-enabled' a digital technology like contact tracing apps is, the more it lends itself to other functions that may contribute to a state's preparation for, or response to, a global health pandemic, such as the use of the data for statistical modelling of the virus as part of public health surveillance, to identify '"clusters" or "hot spots" of the virus'[21] and 'predict [...] the flow of the pandemic and inform [...] preparation and response strategies'.[22] Where data from contact tracing apps is accessible or shared with other state or non-state actors, it may also feed into other public and private sector functions employing AI technologies, given the potential of these apps to track the movements, interactions and associations of whole populations.[23]

18 UN General Assembly, 'Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci – Preliminary evaluation of the privacy dimensions of the coronavirus disease (COVID-19) pandemic' (2020) UN Doc A/75/147 (discussing the range of different models developed).

19 Patrick Howell O'Neill, Tate Ryan-Mosley and Bobbie Johnson, 'Covid Tracing Tracker – a flood of coronavirus apps are tracking us. Now it's time to keep track of them' (2020) MIT Technology Review; Samuel Lalmuanawma, Jamal Hussain, Lalrinfela Chhakchhuak, 'Applications of machine learning and artificial intelligence for Covid-19 (SARS-CoV-2) pandemic: A review', (2020) 139 Chaos, Solitons and Fractals.

20 Lin *et al.* (n 17); Israel Edem Agbehadji, Bankole Osita Awuzie, Alfred Beati Ngowi and Richard C. Millham, 'Review of Big Data Analytics, Artificial Intelligence and Nature-Inspired Computing Models towards Accurate Detection of COVID-19 Pandemic Cases and Contact Tracing', (2020) 17 International Journal of Environmental Research and Public Health.

21 Raju Vaishya, Mohd Javaid, Ibrahim Haleem Khan, Abid Haleem, 'Artificial Intelligence (AI) applications for COVID-19 pandemic', (2020) 14 Diabetes & Metabolic Syndrome: Clinical Research & Reviews; Agbehadji *et al.* (n 20).

22 Lin *et al.* (n 17). Barry Sookman, 'AI and contact tracing: How to protect privacy while fighting the COVID-19 pandemic' (Macdonald-Laurier Institute, 2020) available at <https://macdonaldlaurier.ca/files/pdf/20200416_COVID-Privacy_Sookman_COMMENTARY_FWeb.pdf> 2.

23 Alex Akinbi, Mark Forshaw and Victoria Blinkhorn, 'Contact tracing apps for the COVID-19 pandemic: a systematic literature review of challenges and future directions for neo-liberal societies', (2021) 9 Health Information Science & Systems, 7.

Thus, depending on their design and governance, they offer ways to inform strategies to contain and prevent the further spread of the virus but also pose immediate and long-term risks to human rights, including by diverting resources and focus away from the development of more complex public health strategies in favour of 'technosolutionism', and by opening a gateway for the expansion and normalisation of surveillance technologies and the role of private actors within the public sector. When mandatorily required and used within a system using machine learning techniques, at their most extreme, they potentially provide unprecedented near whole population data on movements and associations ripe for behavioural profiling and fueling predictive analytics within both the public and private sector. The case study of contact tracing apps reveals the challenges that arise in seeking to implement general standards, such as the Siracusa Principles to specific uses cases, particularly in fully identifying and mitigating current and future risk. Rather, where states acknowledged risk, they tended to focus on privacy and the role of data protection legislation, which as discussed in this article, offers important, but incomplete, protection to human rights.

The case study of contact tracing apps therefore raises the question of whether dedicated regulation is required to direct states on their use of digital technologies generally and AI specifically during pandemics. This is a complex and multilayered question, particularly as the use of these technologies by states during pandemics cannot be abstracted from their broader use in the public sector. The question therefore needs to be approached from the intersecting angles of the regulation of disasters – of which pandemics are a part – and the regulation of digital and AI technologies in the public sector. As a contribution to the live and ongoing scholarly and policy debates on digital and AI regulation and standard-setting on global health pandemics, this article proposes a baseline requirement for regulation that cuts across both regulatory environments to enhance transparency and scrutiny of digital technologies prior to roll-out, and their monitoring and review, if adopted.

In Part 2, I identify states' due diligence obligations during disaster, locating digital, including AI technologies, within the measures states may adopt. I then outline the framework contained in the Siracusa Principles to illustrate the general approach expected of states to limit the impact of such measures on other human rights and explain how that framework theoretically supports states in their consideration of these technologies during disaster. In Part 3, I turn to the example of the digitisation of contact tracing to highlight the layered risks to human rights posed by contact tracing apps depending on their design and governance, both in the context of the pandemic and in the longer term, and the protection gaps that emerged during the pandemic as a result

of a failure to systematically engage with these risks. In Part 4, I examine how these protection gaps might be addressed. Without suggesting a complete solution, I highlight the critical role of a process-driven model of transparency, monitoring and oversight to triggering greater use of existing accountability structures and feeding into, and shaping, current regulatory debates.

2 Is There an Obligation to Employ Digital Technologies, Including AI, in Disaster Prevention or Mitigation?

As set out in the introduction, COVID-19 presents high risks to the rights to health and to life. On 30 January 2020, the Director General of the World Health Organization declared a public health emergency of international concern under the International Health Regulations.[24] In this part of the article, I outline the three bodies of law obligating states to take specific measures to protect life: the International Health Regulations, international disaster law, and international human rights law. I examine whether these sources of international law foresee or require the deployment of digital technologies, including AI, as part of how states deal with a global health pandemic and the limitations in place to prevent and mitigate any adverse human rights impacts through such deployment.

2.1 *Three Frames Obligating States to Employ Measures to Protect the Rights to Health and Life and the Role of AI Technologies Therein*

Three bodies of international law require states to take measures to prevent and prepare for disaster and to respond where it occurs. First, the 2005 International Health Regulations require states to 'develop, strengthen and maintain (…) the capacity to respond promptly and effectively to public health risk and public health emergencies of international concern'.[25] Articles 5 and 13 of these Regulations, alongside Annex 1, obligate states to 'develop predefined core capacities in order to be better prepared for health emergencies'.[26] These capacities include surveillance. Article 13 also enables the World Health

24 World Health Organization, 'Archived: WHO Timeline – Covid-19' (27 April 2020), available at: <https://www.who.int/news/item/27-04-2020-who-timeline---covid-19>; Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019-nCoV) (30 January 2020).

25 World Health Organization, International Health Regulations, Third Edition (2005), Article 13(1).

26 Giulio Bartolini, 'The Failure of 'Core Capacities' under the WHO International Health Regulations', (2021) 70 International and Comparative Law Quarterly, 233.

Organization to provide guidance to states in realising these capacities,[27] and Article 18 offers an illustrative list of the types of measures that can be taken to limit the spread of disease. Building on the International Health Regulations, a group of heads of state have called for the adoption of an international pandemic treaty 'for pandemic preparedness and response' which is now under consideration following a special session of the World Health Assembly.[28]

Second, Article 3(a) of the International Law Commission's draft Articles on the Protection of Persons in the Event of Disasters defines a disaster as 'a calamitous event or series of events resulting in widespread loss of life, great human suffering and distress, mass displacement, or large-scale material or environmental damage, thereby seriously disrupting the functioning of society'.[29] Antonio Coco and Talita de Souza Dias argue that this definition of disaster encompasses global health pandemics.[30] Giulio Bartolini characterises the initial assemblage of international disaster law as a 'potpourri of binding instruments'[31] with Sandesh Sivakumaran observing that 'the piecemeal nature of the law has meant that there is little clarity on the rights and obligations of the state affected by the disaster, of the individuals affected by the disaster or of those seeking to provide assistance'.[32] However, both Bartolini and Sivakumaran note that the ILC's Draft Articles and other soft law principles have synthesised and advanced existing norms to introduce greater materiality to states' obligations in relation to disasters.[33]

27 *Ibid.*, 238 (discussing this guidance further).

28 World Health Organization, 'Special session of the World Health Assembly to consider developing a WHO convention, agreement or other international instrument on pandemic preparedness and response' WHA74(16) 31 May 2021.

29 International Law Commission, 'Draft Articles on the Protection of Persons in the Event of Disasters' (2016).

30 Coco and de Souza Dias (n 1) 218.

31 Giulio Bartolini, 'A Universal Treaty for Disasters? Remarks on the International Law Commission's Draft Articles on the Protection of Persons in the Event of Disasters', (2017) 99 International Review of the Red Cross, 1104 (describing 'the legal landscape pertaining to prevention and response to disasters is composed of a "pot pourri" of binding instruments with varying impacts').

32 Sandesh Sivakumaran, 'Techniques in International Law-Making: Extrapolation, Analogy, Form and the Emergence of an International Law of Disaster Relief' (2017) 28 European Journal of International Law, 1105.

33 Bartolini (n 31), discussing the role of the draft articles in particular; Sivakumaran (n 32) 1105 onwards, emphasising the role of the ILC as well as the International Federation of Red Cross and Red Crescent Societies, particularly through the Guidelines for the Domestic Facilitation and Regulation of International Disaster Relief and Initial Recovery Assistance and the Model Act for the Facilitation and Regulation of International Disaster Relief and Initial Recovery Assistance.

In this regard, Article 9(1) of the draft Articles obligates states to 'reduce the risk of disasters by taking appropriate measures, including through legislation and regulations, to prevent, mitigate and prepare for disasters'. The Commentary to the draft Articles clarifies that 'appropriate measures' signify 'specific and concrete measures aimed at prevention, mitigation and preparation for disasters (…) to be evaluated within the broader context of the existing capacity and availability of resources of the State in question'[34] at the 'pre-disaster phase'.[35] Article 9(2) divides the measures into 'the conduct of risk assessments; the collection and dissemination of risk and past loss information; and the installation and operation of early warning systems'.[36] Article 10 of the draft Articles addresses disaster response, setting out 'the duty [of the state] to ensure the protection of persons and provision of disaster relief assistance in its territory, or in territory under its jurisdiction or control'. However, unlike Article 9, the Articles and Commentary do not provide detail on the measures expected of states in response to disaster. Other international instruments such as the IFRC Guidelines for the Domestic Facilitation and Regulation of International Disaster Relief and Regulation of International Disaster Relief and Initial Recovery Assistance also refer to the state's duty to protect and provide relief assistance but focus more on humanitarian relief, including through international assistance, rather than specifying the nature of measures states should take to fulfil the duty to protect.[37] In this regard, international legal instruments on disaster law provide less detail on the importance of preventive and mitigation measures during a disaster to prevent further spread and harm and to bring the disaster to an end.

Third, international human rights law imposes positive obligations on states 'to adopt any appropriate laws or other measures to protect life from all reasonably foreseeable threats, including from threats emanating from private persons and entities'.[38] It also obligates states to 'take positive measures that

34 At para. 11.

35 At para. 15.

36 At para. 17.

37 Available at <https://disasterlaw.ifrc.org/media/1327>.

38 UN Human Rights Committee, 'General Comment No. 36 – Article 6: right to life', CCPR/C/GC/36 (3 September 2019) para. 18; *Öneryildiz v Turkey*, Application No. 48939/99 European Court of Human Rights, (30 November 2004) para. 71 (noting the 'positive obligation on States to take appropriate steps to safeguard the lives of those within their jurisdiction') and para. 90 (where the state 'knew or ought to have known that there was a real and immediate risk to' life, it is under an obligation to take 'preventive operational measures as were necessary and sufficient to protect those individuals').

enable and assist individuals and communities to enjoy the right to health',[39] including to take all necessary steps to '[prevent], [treat] and control (…) epidemic, endemic, occupational and other diseases'.[40] Other international human rights instruments require states to protect particular groups in the context of disaster. For example, Article 11 of the UN Convention on the Rights of Persons with Disabilities requires states to take 'all necessary measures to ensure the protection and safety of persons with disabilities in situations of risk, including situations of armed conflict, humanitarian emergencies and the occurrence of natural disasters'.

Marie Aronsson-Storrier documents the influence of international human rights law on the framing of Article 9 of the ILC's Draft Articles, observing that disaster risk reduction had previously failed to focus on states' positive obligations to prevent and mitigate disaster.[41] Similarly, international and regional bodies vested with responsibility for the authoritative interpretation and application of international human rights law pay increasing attention to disasters within their mandates.[42] However, other commentators argue that the three bodies of international law insufficiently interact, leading to potential protection gaps.[43] For example, Brigit Toebes *et al.* argue for greater systemic integration and regime interaction between international human rights law, specifically the right to health, and the International Health Regulations.[44]

Antonio Coco and Talita de Sousa Diaz typologise states' due diligence obligations across the three frameworks set out above (as well as under international humanitarian law) as '1) capacity-building and preparedness 2) monitoring and reporting 3) response and mitigation 4) international cooperation'.[45] However, none provide an exhaustive list or address the possible role(s) of

39 UN Committee on Economic, Social and Cultural Rights, 'General Comment No. 14 – The Right to the Highest Attainable Standard of Health', E/C.12/2000/4 (11 August 2000) para. 37.

40 ICESCR Article 12(2)(c) of the International Covenant on Economic, Social and Cultural Rights. See, UN Committee on Economic, Social and Cultural Rights, *ibid*, para. 16.

41 Marie Aronsson-Storrier, 'Sendai Five Years on: Reflections on the Role of International Law in the Creation and Reduction of Disaster Risk', (2020) 11 International Journal of Disaster Risk Science, 234.

42 Elizabeth Ferris, 'How Can International Human Rights Law Protect Us from Disasters?', (2014) 108 American Society of International Law, 177–180.

43 Pratik Dixit, 'Synergising International Public Health Law and International Disaster Law', (2020) European Journal of Risk Regulation, 1.

44 Brigit Toebes, Lisa Forman, and Giulio Bartolini, 'Toward Human Rights-Consistent Responses to Health Emergencies: What Is the Overlap between Core Right to Health Obligations and Core International Health Regulation Capacities?', (2020) 22 Health and Human Rights Journal 99.

45 Coco and de Souza Dias (n 1) 226–235.

digital technologies within the measures foreseen to meet states' obligations. The only international standard to envisage a role for technology is the Committee on Economic, Social and Cultural Rights (CESCR) which requires states to 'make available relevant technologies, using and improving epidemiological surveillance and data collection on a disaggregated basis' as part of its approach to fully realise the right to health through '[t]he prevention, treatment and control of epidemic, endemic, occupational and other diseases' under Article 12(2)(c) of the International Covenant on Economic, Social and Cultural Rights.[46]

At least currently, the international legal sources available do not appear to require states to employ digital technologies within disaster prevention or mitigation strategies. The position of the European Court of Human Rights strengthens this assumption in noting that, 'the choice of means is in principle a matter that falls within the Contracting State's margin of appreciation' and that 'even if the State has failed to apply one particular measure provided by domestic law, it may still fulfil its positive duty by other means'.[47] However, international law also does not prohibit the use of digital technologies.[48] In this respect, as noted in the introduction, the WHO anticipated that digital technologies, including AI, would play a key role in the pandemic.[49] This expectation was mirrored by others who emphasised the role of digital technologies in facilitating communications and social connection; remote healthcare, work and education; data analysis on the spread, resource allocation, and mitigation measures; and to develop vaccines and treatment.[50] Moreover, as states

46 CESCR (n 39) para. 16.

47 European Court of Human Rights, *Budayeva and Others v Russia*, Applications nos. 15339/02, 21166/02, 20058/02, 11673/02 and 15343/02 (29 September 2008) para. 134; see also Coco and de Souza Dias (n 1) 220 (discussing the '[inherent] flexibility of due diligence obligations).

48 However, prohibitions over the use of certain AI technologies are currently being considered within the Artificial Intelligence Act by the European Commission (n 10).

49 Artificial Intelligence and Covid-19 (n 7) although, notably, many of the articles emphasise the legal, ethical, and equality implications of AI technologies.

50 See, for example, Swami Sivasubramanian, 'How AI and Machine-Learning are Helping to Fight COVID-19', World Economic Forum (28 May 2020); Access Now, 'Recommendations on Privacy and Data Protection in the Fight against Covid-19', 4 (observing that 'public authorities should be able to rely on data, including health data, to determine the best course of action to mitigate the spread of the virus and identify what measures must be taken to safeguard people and their rights during and after the crisis' but noting that, '[m]easures applied should be transparent, necessary and proportionate and, when they exist, data protection and privacy laws should have clear exceptions that apply to public health crises to allow for greater use of data than usual'); Marcello Ienca and Effy Vayena, 'On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic', (2020)

and other actors increasingly employ digital technologies, it is possible that the interpretation of states' due diligence obligations may evolve due to 'new scientific or technological knowledge'.[51] Thus, international law could become less deferential to states' choices and assessments of effective measures to take as a result of technological development or availability.[52] However, the extent to which international law assumes a more prescriptive stance is likely to be predicated on the quality of evidence available to show that a particular technology could contribute to disaster prevention or mitigation as the role of a particular technology is often accompanied by a lack of detail or speculation rather than clear evidence, and the extent to which it presents an exclusive preventative or mitigating measure, since non-technological solutions capable of fulfilling the same task are often available.

2.2 *Limitations on the Measures Employed*

Notwithstanding the possibility – and potentially the expectation – on states to consider deploying digital technologies as part of their due diligence obligations within a pandemic, as is now well documented, many forms of digital technologies, particularly AI, present risks to the rights to privacy and non-discrimination, the levels of which vary depending on their design, regulation, and oversight.[53] Further risks to human rights arise from the purpose or context in which the technologies are deployed. Accordingly, even where digital technologies potentially offer ways in which to protect human rights, such as the rights to life and health during a global health pandemic, they may also present threats to many other human rights, as discussed further in Part 3 of this article. How international law deals with the dual role of technologies that may simultaneously act as vehicles for the protection of human rights, while presenting threats to them, becomes critical to analysis of whether they should form part of the measures adopted by states to meet their due diligence obligations under international law.

No dedicated standards provide direction to states on the use of digital or AI technologies in preventing and mitigating harm during global health

26 Nature Medicine 463; Ada Lovelace Institute, 'No Green Lights, No Red Lines: Public Perspectives on COVID-19 Technologies', (July 2020) 4.

51 International Tribunal for the Law of the Sea (ITLOS), Seabed Disputes Chamber, 'Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area', Advisory Opinion, 1/2/2011 (1 February 2011) para. 117.

52 International Law Association Study Group on Due Diligence in International Law, 'Second Report' (July 2016), 3 (discussing how due diligence obligations can evolve, mature and become stricter over time).

53 See sources cited in (n 9).

pandemics or disasters more broadly, although there is increasing attention to what humanitarian principles like "do no harm" mean in the digital age.[54] States' approaches to their due diligence obligations during pandemics cannot be abstracted from their wider use of digital technologies in the public sector, particularly where they have not derogated from their existing international human rights obligations. No dedicated international treaty or national law exists governing the design, development and deployment of digital or AI technologies generally, or within the public sector. However, the UN Human Rights Council has issued a number of relevant resolutions, including two on the right to privacy in the digital age,[55] which recognise the risks posed by the use of digital technologies, including AI, to the right to privacy and other human rights and 'recognis[es] the need to apply international human rights law in the design, development, deployment, evaluation and regulation of these technologies, and to ensure they are subject to adequate safeguards and oversight'. In this regard, the 2019 resolution calls upon states to undertake a range of preventative, legislative, oversight, accountability and remedial measures to protect human rights.[56] Similarly, some states have adopted national AI strategies which to varying degrees make some reference to ethical and human rights principles albeit typically lacking in comprehensiveness or detail.[57] Other multistakeholder initiatives have advanced soft-law principles, again most often offering baseline ethical principles although some, such as the Toronto Declaration, focus on human rights.[58] Further, regional bodies, such as the European Commission, are currently exploring forms of regulation with the EU Artificial Intelligence Act in draft form and reflecting the most detailed attempt at regulation of digital and AI technologies, including coverage of 'prohibited artificial intelligence practices' and 'high-risk AI systems'.[59]

Other pieces of regulation, such as the EU General Data Protection Regulation (GDPR), cover some aspects of use in their focus on data processing. Given the reliance of digital technologies and AI technologies in particular on data, specific rules on data processing reflect a critical component of the

54 Alexandrine Pirlot de Corbion, Dr Gus Hosein, Dr Tom Fisher, Ed Geraghty, Ailidh Callander, Tina Bouffet, 'The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Age' (2018); Jo Burton, '"Doing No Harm" in the Digital Age: What the Digitalization of Cash Means for Humanitarian Action', (2021) International Review of the Red Cross, 102.

55 See (n 11).

56 *Ibid.*

57 See (n 12).

58 Amnesty International and Access Now, 'The Toronto Declaration: Protecting the Right to Equality and Non-Discrimination in Machine Learning Systems' (16 May 2018).

59 See (n 10).

protection of human rights. The EU General Data Protection Regulation specifies core principles of 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation', 'integrity and confidentiality' and 'accountability'.[60] It provides procedural rights for individuals to support the enforcement of rights, such as the right to erasure;[61] sets out concrete steps and processes for data controllers to assess the potential impact of data processing on 'the rights and freedoms of natural persons', such as requirements to carry out data protection impact assessments where data processing poses a high risk to such rights and freedoms;[62] and establishes national supervisory bodies to play a monitoring and oversight role in relation to data processing.[63]

However, not all countries have enacted data protection legislation. Moreover, data protection legislation does not comprehensively deal with the issues raised by digital technologies and particularly AI. Its coverage is not complete in its treatment of data. For example, it does not address bias in training or input data.[64] Regulation like the EU GDPR focuses on the individual impact of data processing but not the collective impact of such activities on society or the impact on groups.[65] Data protection also only addresses data processing. It therefore only focuses on one part of the design, development and deployment of digital technologies, rather than the full 'socio-technological system'.[66] There are therefore many dimensions to public sector use of digital, including AI, technologies that fall outside of its scope. For example, the GDPR provides

60 General Data Protection Regulation, setting out the Principles, art. 5. See also, Article 9 which addresses the processing of special categories of data which includes health data. Article 9 prohibits the processing of such data, unless one of the exceptions in Article 9(2) apply.

61 Art. 17.

62 Art. 35.

63 Art. 51.

64 See, for example, Solon Barocas and Andrew D. Selbst, 'Big Data's Disparate Impact', (2016) 104 California Law Review 671; Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial General Classification', (2018) 81 Proceedings of Machine Learning Research, 1; Eirini Ntoutsi, 'Bias in data-driven artificial intelligence systems – An introductory survey', WIREs Data Mining Knowl Discov (2020).

65 Reuben Binns *et al.*, 'Equality Task Force: Mind the Gap: How to Fill the Equality and AI Accountability Gap in an Automated World', Institute for the Future of Work (October 2020) 32, noting that '[d]ata protection law is aimed at protecting people from risks arising as a result of the processing of their personal data, and offers individuals legal rights in prescribed circumstances. It is not aimed at countering novel forms of collective harm or the projection of group-based structural inequalities into the future'.

66 *Ibid.*, 27.

protection for fully automated decisions[67] but not the more common situation in which AI technologies are used to support decisions, such as the use of algorithmic risk assessments in decision-making.[68] It also does not cover choices to use digital or AI technologies in the first place; how determinations are made on the necessity and proportionality of the use of technologies, including against non-technological approaches; transparency on the fact and reasons for their use; or how digital technologies are procured and the involvement of the private sector in public sector decision-making and service delivery. Yet, these dimensions can have significant implications for the protection of human rights.

The lack of dedicated – or complete – regulation does not mean that digital technologies exist in a (partial) legal vacuum. However, how existing frameworks, such as international human rights, public and constitutional law, apply to their design, development and use requires articulation and application. In the context of a global pandemic, the Siracusa Principles are of particular importance as they advance a framework for how states approach restrictions to rights in times of 'pressing public or social need'. Public health constitutes one of the recognised grounds on which rights can be restricted through formal derogation or limitations 'in order to allow a state to take measures dealing with a serious threat to the health of the population or individual members of the population. These measures must be specifically aimed at preventing disease or injury or providing care for the sick and injured'.[69] In the absence of a formal derogation, the Principles provide that in order to establish the necessity of the restriction on a right, the limitation must be prescribed by a 'clear and accessible' law,[70] be 'based on one of the grounds justifying limitations recognized by the relevant article of the Covenant'; 'respond to a pressing public or social need'; 'pursues a legitimate aim'; and meet the requirements of proportionality.[71] The Principles provide that, '[i]n applying a limitation, a state shall use no more restrictive means than are required for the achievement

67 Art. 22.

68 For a discussion of the role of risk assessments, see, Alicia Solow-Niederman, YooJung Choi and Guy Van den Broeck, 'The Institutional Life of Algorithmic Risk Assessment', (2019) 34 Berkeley Tech. L.J., 705.

69 American Association for the International Commission of Jurists, 'Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights' (1985) para. 25.

70 *Ibid.*, at paras. 15–18.

71 *Ibid.*, Part I(A)(10).

of the purpose of the limitation',[72] must not undermine the 'essence of the right'[73] and 'adequate safeguards and effective remedies' must be available.[74]

While the Principles are not technology-specific, theoretically at least, they provide a framework for states both to consider digital technologies within their wider due diligence obligations ahead of, and during, a disaster while ensuring the least restrictive impact on other human rights. However, as discussed in the next part of this article, in the context of the COVID-19 pandemic, there is very little evidence of states adopting this methodological approach to the use of digital or AI technologies. This raises the question of whether dedicated regulation is required on the use of digital technologies in disaster contexts to complement the partial dedicated coverage of data protection legislation and to enhance implementation of general standards. This question is addressed in the final part of this article. In the next section, I illustrate the depth and breadth of potential human rights risks posed by the use of digital technologies, particularly when AI is involved, through the case study of contact tracing apps and reflect on the implications of the lack of a dedicated regulatory framework of digital technologies in the context of a global health pandemic or within the public sector more broadly.

3 The Digitisation of Contact Tracing via Apps

Contact tracing reflects an established strategy in public health surveillance,[75] with the International Health Regulations foreseeing it as one of a range of possible measures to contain the spread of a virus, such as COVID-19.[76] It can thus be understood both as a disaster risk reduction measure to prevent the emergence of a health pandemic as well as part of disaster response to prevent the further spread of a virus. It typically involves an individual diagnosed or exposed to a virus providing healthcare professionals with a list of recent contacts so that they can contact these individuals and provide advice on action they need to take, for example, to self-isolate or arrange for testing. As

72 *Ibid.*, para. 11.

73 *Ibid.*, para. 2.

74 *Ibid.*, para. 18.

75 World Health Organization, 'Coronavirus Disease (COVID-19): Contact Tracing' (28 July 2020); Benjamin Armbruster & Margaret L. Brandeau, 'Contact tracing to control infectious disease: when enough is enough', (2007) Health Care Manage Sci 10, 342 (referring to contact tracing as a 'primary means of disease control for infectious diseases with low prevalence').

76 Arts. 18(1) and 23(1).

contact tracing traditionally relies on memory, knowledge of the identity of everyone with whom a person has had contact, and a willingness to impart that information, it has inherent shortcomings.[77] It also requires significant human capacity to deliver a quick and effective service. At the beginning of the COVID-19 pandemic, contact tracing apps were quickly developed as a means of digitising human contact tracing. While states rarely advanced a specific justification for the introduction of the apps, they were assumed to complement human contact tracing.[78] In theory, therefore, contact tracing apps appeared well-positioned to form part of a state's response to the pandemic and therefore protect life and health. However, as quickly became apparent, contact tracing via an app is a qualitatively different exercise to simply digitising a human function and raises many new human rights issues. As discussed in this section, contact tracing apps, even in purely digital form, introduce different human rights issues to those posed by human contact tracing which are also 'privacy-intrusive'.[79] When employed within a system using machine learning techniques on the data gleaned, these risks are accentuated, particularly as contact tracing apps potentially offer unprecedented insights into population movements and interactions.

In this part of the article, I group the risks into three sets: first, direct risks emanating from the design and access to an app; second, the risk that technology dominates or distorts the formulation of public health strategies and thus detracts from the adoption of other measures to address a pandemic; and third, the risks of mission creep and repurposing, including into broader AI systems, within the context of the COVID-19 pandemic and beyond. Whether these risks attach to a particular contact tracing app depends on its design, operating system, the nature of wider system within which it is placed, and whether it includes the use of AI technologies, the potential for sharing and access to data, as well as mission and function creep and the governance system in place. Particularly at the outset of the pandemic, it was not always possible to fully engage with the model proposed or adopted and even now, it can be difficult to ascertain the role of AI, for example, within a particular system. The breadth and scale of these risks highlights the importance of applying frameworks such

77 Isobel Braithwaite *et al.*, 'Automated and Partly Automated Contact Tracing: A Systematic Review to Inform the Control of COVID-19' (2020) 2 The Lancet Digital Health, 607.

78 For a study into the use of contact tracing apps, see 'Contact Tracing Apps: A New World for Data Privacy', Norton Rose Fulbright (February 2021), surveying the use of contact tracing apps in 17 countries.

79 UN General Assembly, 'Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci – Preliminary evaluation of the privacy dimensions of the coronavirus disease (COVID-19) pandemic' (2020) UN Doc A/75/147, paras. 18–20.

as the Siracusa Principles. However, in practice these principles did not feature centrally within states' responses which tended to either fail to address the risks to human rights or focus on privacy and data protection frameworks leading to potential protection gaps.

3.1 *Immediate Human Rights Risks of Digitising Contact Tracing*

The digitisation of contact tracing raised a wide range of human rights concerns. The first set of concerns arose from the system adopted.[80] Risks to privacy were identified where models relied on data capable of directly identifying an individual, including through location,[81] proximity, or interaction data.[82] These risks were heightened where data was stored on a central database rather than decentralised through storage on a person's device.[83]

In states lacking strong data protection legislation, commentators argued that the impact of contact tracing on human rights was particularly severe. For example, in a report on Kenya and Uganda, Sigi Waigumo Mwanzia *et al.*, reported that,

> [i]n both countries, existing and new surveillance measures were used to 'track and trace' individuals suspected to have or who had contracted the COVID-19 virus. These measures were deployed in environments where compliance with legal and human rights standards was inadequate, which heightened the risk of human rights violations (…) These include poor oversight over COVID-19 data collection; lack of independent data protection authorities; disclosure of personal data without consent; the use of telecommunications data to 'track and trace' individuals; surveillance of public spaces using CCTV and biometric technologies; broad search powers to medical and public health officers; and the lack of transparency and accountability by state and non-state actors.[84]

80 For a discussion of design options, see, Ada Lovelace Institute, 'Exit Through the App Store?' (20 April 2020) 21.

81 Access Now (n 50) 9, discussing the 'highly revealing' nature of location data.

82 'Apple and Google Announced a Coronavirus Tracking System. How Worried Should We Be?' (<aclu.org>).

83 See, Amnesty International, 'Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy' (16 June 2020) available at <https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/>, surveying the human rights risks posed by different contact tracing apps introduced in different countries.

84 Sigi Waigumo Mwanzia, Victor Kapiyo, and Phillip Ayazika, 'Unseen Eyes, Unheard Stories', ARTICLE 19 Eastern Africa, the Kenya ICT Action Network and Pollicy (2021).

Connected to these questions, were questions of whether contact tracing apps would be introduced on a voluntary or mandatory basis. A mandatory requirement to use contact tracing apps raised clear human rights risks through digital surveillance, particularly if capable of identifying individuals and with whom they associate. However, concerns were also raised that the voluntary uptake of apps could become a de facto requirement for certain individuals, if required to access public spaces, work, or education[85] or for certain groups, such as migrant workers.[86] Both contexts raised further risks of discrimination due to ongoing digital divides and the inability of some people, often in already marginalised positions, to access digital apps.

3.2 *Impact of Focus on Contact Tracing Apps on Wider Due Diligence Obligations*

In addition to the direct human rights risks posed by contact tracing apps, commentators also pointed to the potential that a focus on technology could detract from the development of multilayered strategies to dealing with the pandemic.[87] These points were made on two levels. First, organisations such as the American Civil Liberties Union pointed out that the use of digital technologies still had to be embedded within a broader pubic health strategy, noting that the effectiveness of such technologies 'is predicated on the availability of widespread, affordable, and prompt testing, so it would be pointless to deploy automated contact tracing at the expense of traditional medical and social interventions'.[88] Second, commentators such as Ross Anderson questioned whether the focus on contact tracing apps reflected an example of techno-solutionism or 'do-something-itis'[89] in place of more complex, multi-layered strategies to address the pandemic. He observed that even if contact tracing apps present part of the solution, '[w]e must not give policymakers the false

85 Patrick Howell O'Neill, 'India is Forcing People to Use its Covid App, Unlike Any Other Democracy', MIT Technology Review (7 May 2020) available at <https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/>.

86 Sharifah Sekalala, Stéphanie Dagron, Lisa Forman and Benjamin Mason Meier, 'Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis', (2020) 22/2 Health & Human Rights Journal, 7 (arguing that in Singapore 'employers are told to encourage all workers to download the TraceTogether app, but it is mandatory for certain groups of migrant workers, making them particularly vulnerable as they often have fewer rights than other citizens').

87 Algorithm Watch, 'Automated decision-making systems and the fight against COVID-19 – our position' (April 2020).

88 Daniel Khan Gillmor, 'ACLU Principles for Technology-Assisted Contact-Tracing' (16 April 2020).

89 Ross Anderson, 'Contact Tracing in the Real World', Light Blue Touchpaper (12 April 2020).

hope that techno-magic might let them avoid the hard choices' of resource allocation to public health.[90]

3.3 *Risks of Repurposing and Mission Creep via Apps*

The third set of risks identified with contact tracing apps related to the potential for mission creep, through the repurposing of the apps away from a sole function of contact tracing to serve other goals of the state, pandemic-related, or otherwise. Reports of mission creep in the use of the app for surveillance purposes have already been alleged in some countries where the model adopted was not decentralised (meaning the data was stored locally on a person's device) or anonymised. For example, the Social Science Research Council reported data from the app introduced in Singapore initially 'could be accessed by law enforcement to support criminal investigations' but following public opposition was then limited 'to specific cases involving "serious offenses", such as kidnapping or terrorism'.[91]

As discussed above, the data gleaned from contact tracing apps has the potential to support statistical modelling of the virus, and thus could potentially be repurposed for public health surveillance where stored centrally. Given the growing role of AI technologies in the public sector and the unprecedented and unique information potentially revealed by contact tracing apps, particularly where the data is held on centralised systems, and is either not anonymised or capable of being reidentified, mission creep could not only accelerate but also transform the nature of existing – and future – uses of AI within the public sector, such as behavioural profiling, targeting, and the use of predictive analytics within decision-making, including in major life events.[92]

Concerns over function creep have also been raised in relation to the expansion of apps to register vaccination status. The underlying activity of using vaccine certificates to restrict or permit movement – particularly outside of international travel where some states already require proof of receipt of certain vaccinations – does not have the same established history as human

90 *Ibid.* See also, Javier Ruiz, 'Contact-Tracing Apps: No Substitute for Public Health Care Interventions', Bot Populi (21 April 2020).

91 Social Science Research Council, 'Surveillance and the 'New Normal' of Covid-19: Public Health, Data, and Justice' (2021) 16; Sekalala et al (n 86), alleging that a number of countries 'have reportedly used the COVID-19 pandemic as an opportunity to analyze telecommunications data under the guise of "contact tracing"'.

92 UN General Assembly, 'Final report of the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health, Dainius Pūras – Commentary on the COVID-19 pandemic' (2020) UN Doc A/75/163, at paras. 85–86 (noting that technologies such as 'digital tracing tools' when linked to AI systems such as 'social credit scoring' can '[break] down trust in society').

contact tracing. It raises clear risks of discrimination, particularly including where vaccines are not equally available and accessible.[93] Discrimination could also arise if 'vaccine passports were linked to rights or used to track populations, already marginalised groups could potentially be subject to more scrutiny such as by police, employers or health checks on vaccine status'.[94] Civil society organisations have also expressed concern that vaccine certificates could become a national[95] or even global identity document[96] if vested with 'multiple uses (e.g. access to services) in multiple domains (i.e. public sector, private sector), in multiple countries (i.e. travel)'[97] and create 'long-term infrastructure in response to a time-bounded crisis' alongside '[s]cope creep and information flows'.[98] These concerns underscore the importance of debate and scrutiny of the role of vaccine certificates, yet, the digitisation of vaccine certificates, including through expansion on the same app originally built for contact tracing, may elide the substantial differences in the two underlying activities by rather turning the focus to the possession of apps which permit (or deny) freedom of movement.

In addition to direct mission creep, commentators expressed concern about the potential for digital technologies such as contact tracing apps to result in the normalisation of surveillance technologies beyond the pandemic. At the outset of the pandemic, Yuval Harari raised concerns about the role of 'biometric surveillance as a temporary measure' becoming normalised post-pandemic, noting that 'temporary measures have a nasty habit of outlasting

93 Civil Liberties Union for Europe, 'Digital Green Certificate: Concerns with the European Commission's Proposal for a Regulation and Suggestions for Amendment' (2021) <https://dq4n3btxmr8c9.cloudfront.net/files/3UNqy8/Liberties_Digital_Green_Certificate_PolicyBrief.pdf>; The Royal Society, 'Twelve criteria for the development and use of COVID-19 vaccine passports' (14 February 2021) <https://royalsociety.org/-/media/policy/projects/set-c/set-c-vaccine-passports.pdf>; Ada Lovelace Institute, 'What place should COVID-19 vaccine passports have in society?' (17 February 2021) <https://www.adalovelaceinstitute.org/summary/covid-19-vaccine-passports/>.

94 Royal Society, *ibid.*

95 Big Brother Watch, 'Stop Covid Passes' Campaign <https://bigbrotherwatch.org.uk/campaigns/stopvaccinepassports/>.

96 "Anytime and anywhere": Vaccination passports, immunity certificates, and the permanent pandemic Privacy International (17 December 2020) <https://privacyinternational.org/long-read/4350/anytime-and-anywhere-vaccination-passports-immunity-certificates-and-permanent>.

97 *Ibid.*

98 Ada Lovelace Institute, 'What place should COVID-19 vaccine passports have in society?', Rapid expert deliberation (17 February 2021).

emergencies'.[99] Others highlight the risks to 'future privacy', asking 'will full privacy protections be reinstated after the epidemic?'.[100]

Moreover, commentators also raised concerns about mission creep through the increasing role of technology and technology companies in the health – and public – sector as a result of COVID-19. Given the manifold roles of technology during the pandemic, this point encompasses, but goes wider than, contact tracing apps. For example, Rajat Khosla points to the marketisation of health data in a sector in which the business model of many companies is the purchase and sale of 'people's digital data (…) as a commodity' in a 'generally thinly regulated marketplace in data'.[101] Sharifah Sekalala et al also locate contact tracing apps within a 'massive accelerat[ion] (…) toward new digital technologies in health' in the course of the pandemic,[102] highlighting expansions in public-private partnerships including with technology companies that have been the subject of criticism for the human rights impact of their data practices, alongside risks of 'unsupervised experimentation'.[103] Moreover, Access Now points to the reliance on technology companies during COVID-19 as another example of the increasing dependency of public actors on private actors 'to function'.[104] It argues that, 'governments may enhance the powers of dominant platforms, exacerbate the risks associated with data

99 Yuval Noah Hariri, 'The World After Coronavirus', Financial Times (20 March 2020) <https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75>.

100 Michael J Parker, Christophe Fraser, Lucie Abeler-Dörner and David Bonsall, 'Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic' (2020) 46 Journal of Medical Ethics, 427–431. See also, UN Human Rights Council, 'Report of the Independent Expert on human rights and international solidarity, Obiora Chinedu Okafor on International solidarity in aid of the realization of human rights during and after the coronavirus disease (COVID-19) pandemic' (2021) UN Doc A/HRC/47/31, para. 20 (describing centralised databases in particular as a 'long term threat to human rights').

101 Rajat Khosla, 'VIEWPOINT: Technology, Health and Human Rights: A Cautionary Tale for the Post-Pandemic World', (2020) 22 Health and Human Rights Journal, 63.

102 Sekalala *et al.* (n 86); see also, Michael Veale, 'Sovereignty, privacy and contact tracing protocols' in Linnet Taylor, Gargi Sharma, Aaron Martin, and Shazade Jameson (eds), Data Justice and COVID-19: Global Perspectives (Meatspace Press 2020), discussing, '[t]he drama of contact tracing applications has laid bare how much of both extractive and protective infrastructure is reliant on the choices of a small number of gargantuan corporations'.

103 For discussions on experimentalism, see also, Rafael Evangelista and Rodrigo Firmino, 'Modes of Pandemic Existence: Territory, Inequality and Technology' in Linnet Taylor *et al.* (n 102) 103, arguing that the 'current crisis enables an experimental setting for big technology companies'.

104 Access Now (n 50) 15.

harvesting and monetisation of health information, and legitimise privacy-invasive services'.[105]

Accordingly, significant concerns have been raised about the potential for contact tracing apps to create an infrastructure for future surveillance and to facilitate the embedding of private sector actors within the public sector.

3.4 *Application of IHRL Standards to the Use of Contact Tracing Apps*

The foregoing highlights the wide-ranging current and future risks posed by the use of contact tracing apps in the context of the COVID-19 pandemic, whether in purely digital form or as part of a system using AI techniques, that go well beyond the direct privacy implications of a particular technological model, and the consequent importance of a full assessment not only of risk but also of the adequacy and effectiveness of existing regulation. As discussed in Part 2, from a human rights perspective, existing standards, particularly the Siracusa Principles, provided states with a methodological approach to assess whether and how they could introduce contact tracing apps as part of their wider due diligence obligations to protect the rights to life and health,[106] while ensuring the measures had the least invasive effect on other human rights. Many of the human rights issues identified in this section could have been addressed through adherence to the limitation provisions in the Siracusa Principles, even in the absence of formal derogations. However, the Siracusa Principles and the wider IHRL framework did not feature centrally in how states' approached the introduction of contact tracing apps, with the risks to human rights either bypassed or narrowly concentrated around data protection legislation, where in place.[107] This highlights protection gaps through a failure to apply existing human rights obligations to the specific use case of contact tracing as well as the inadvertent narrowing effect data protection legislation can have on the governance of digital technologies more generally.

In the UK, for example, the UK's parliamentary Joint Committee for Human Rights issued a report on contact tracing apps, in which it rejected the government's contention that existing data protection legislation was sufficient to safeguard human rights risks posed by the use of contact tracing. It asserted that

105 *Ibid.*

106 Parker *et al.* (n 100).

107 See, Norton Rose Fulbright (n 78) analysing apps in 17 countries; see also, MIT Technology Review, 'Covid-19 Tracing Tracker', at <https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/> (rating apps for voluntariness; limitations on data use; data destruction; minimisation of data collection; and transparency).

> The current data protection framework is contained in a number of different documents and it is nearly impossible for the public to understand what it means for their data which may be collected by the digital contact tracing system. Government's assurances around data protection and privacy standards will not carry any weight unless the Government is prepared to enshrine these assurances in legislation.[108]

It proposed specific provisions to be contained in dedicated legislation on the use of contact tracing apps, such as purpose and access limitation, local storage and data deletion, prohibition of data reconstruction, regular review and reporting to Parliament on 'the efficacy and privacy protections relating to digital contact tracing' and the establishment of a 'Digital Contact Tracing Human Rights Commissioner for oversight and monitoring'[109] alongside a declaration of compatibility with the Human Rights Act since 'the introduction of this app raises issues that go beyond data protection and privacy. Other human rights which are protected under the Human Rights Act 1998 (HRA) and ECHR are engaged, for example, the right to non-discrimination in employment and immigration matters'.[110] The Committee also anticipated arguments against legislation on the basis of the expediency of the situation but underscored that, 'legislation enshrining assurances in law is perfectly viable in time for the national roll out in the middle of this month'.[111] However, the government rejected the calls for dedicated legislation.

The data protection impact assessment published on the COVID-19 app store organises risks under '[t]ypes of privacy risks', including noting that, the 'context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge'.[112] It recognises '[n]on-compliance with human rights legislation' as a risk but does not provide a full assessment of human rights risks or offer mitigation strategies. While the impact assessment acknowledges the engagement of external data processors, including private companies, it does not provide any information on how they have been vetted or the nature of the agreements in place. Rather, it simply states that they 'have been engaged under contract with NHS England and will have access to the data which is aggregated to required level

108 Joint Committee on Human Rights, 'Human Rights and the Government's Response to Covid-19: Digital Contact Tracing' HC 343 HL Paper 59 (7 May 2020) para. 23.

109 *Ibid.*, para. 23.

110 *Ibid.*, para. 24.

111 *Ibid.*, para. 25.

112 NHS England, 'Data Protection Impact Assessment: NHS COVID-19 Data Store'.

or data which has been de-identified to mitigate the risk of identification of the individual in the data mart'.

In response to the question '[w]ould it be appropriate to seek the views of data subjects or their representatives on the proposed processing?' it states 'no' with the explanation '[v]arious reasons, including the fact that this is large scale processing which needs to be facilitated very quickly to support the emergency response for COVID-19'. It also states that '[s]ubject matter experts are involved in ensuring that the processing meets safe, efficient and effective standards' but does not explain who these experts are, how they were recruited, what their input has been or how it has been used. Rather the assessment leaves the question on 'how this will be done' blank.

As examined in Part 2, data protection only partially covers the human rights risks posed by contact tracing whether in pure digital form or when involving AI. Data protection impact assessments could not therefore fully capture the potential risks to human rights posed by contact tracing apps, and the necessity and proportionality of the app, including within a broader public health strategy, which made it difficult to assess the contribution and intersection of contact tracing apps with other strategies as well as identify any risks of over-investment in these technologies at the expense of other due diligence measures, or the framework in place to prevent future repurposing by the state or companies involved.

Accordingly, how states interpreted and implemented their existing human rights obligations varied. At one end of the spectrum, some states paid almost no attention to the risks to human rights, using the pandemic as an opportunity to develop and expand surveillance tools, including in some cases by centrally collecting data, linking it with other data, and analysing it with machine learning tools. Even where some human rights risks were acknowledged, they tended to be tied to the specificities of data protection frameworks and therefore failed to comprehensively identify and address the full risks to human rights. The experience of contact tracing apps demonstrates the challenges of regulatory environments which are simultaneously very specific (in the form of data protection legislation) and general, requiring states to interpret how general legal provisions apply to specific case studies, such as the use of digital technologies in the public sector during a global health pandemic, and the protection gaps that can result.[113] Such challenges can be aggravated in relation to

113 Algorithm Watch (n 87), arguing that, we should ensure that this debate about COVID-19 surveillance does not happen in a vacuum. Some ADMS, most notably face recognition, already proved to be problematic. The current state of emergency cannot be used to justify their deployment: on the contrary, all issues highlighted during "ordinary" times –

AI technologies, where there may be a 'regulatory disconnect' brought about by 'uncertainty surrounding innovations and their attendant risks and benefits (…) and [a]mbiguity in the application of existing regulations'.[114] In the following section, I consider whether greater articulation of these obligations through standard-setting could contribute to addressing these shortcomings.

4 Regulating Public Sector Use of Digital Technologies, including AI, in Times of Disaster and Beyond

Using the example of contact tracing apps, this article has illustrated the challenges that arise from a lack of dedicated regulation on digital technologies more broadly, and AI specifically, and from dedicated legislation only covering part of the digital ecosystem. Closing these protection gaps presents a more complex question, however, particularly as the political economy of digital technologies, particularly AI, may mean that attempts to legislate result in more permissive regulatory frameworks. Challenges also arise over the form of regulation as on the one hand, regulation of specific technologies can be critiqued as inefficient and incapable of adapting to future iterations of technology, whereas overarching legislation can be viewed as too abstract, raising similar issues to the application of general laws to the use of digital technologies.[115] Moreover, as this article has demonstrated, even when considering one form of technology, such as a contact tracing app, its design, operation, and purpose, may result in different classifications and therefore it being subject to regulation, such as the draft EU Artificial Intelligence Act, or falling outside of it. They also highlight that, as Gary Marchant has recently observed, the regulation of digital technologies is likely to lead to the least bad answer rather than the optimal solution.[116] The identification of regulatory pathways therefore

lack of accuracy, systematic bias in its prescriptions, broader concerns about possible abuses of biometric data etc. – become even more important during exceptional times, when the health and safety of all are at stake. We should not only make sure that this crucial debate is not led by technologists or technologies, but also ensure that the technologies involved are proven to benefit society'.

114 Anna Butenko and Pierre Larouche, 'Regulation for innovativeness or regulation of innovation?', (2015) 7 Law, Innovation and Technology, 52.

115 Sofia Ranchordás and Mattis van't Schip, 'Future Proofing Legislation for the Digital Age' in Sofia Ranchordas and Yaniv Roznai (eds), Time, Law, and Change (Hart 2020) (emphasising two central elements of the future-proof approach: foresight (or anticipation) and adaptability).

116 Gary E. Marchant, 'Governance of Emerging Technologies as a Wicked Problem', (2021) 73 Vanderbilt Law Review, 861.

requires careful consideration rather than an immediate reach for the enactment of comprehensive legislation.

While in the space of this article, it is not possible to delve into a full analysis of the future direction of digital technologies regulation as a whole, some clear regulatory priorities can be identified from the experience of the COVID-19 pandemic, and contact tracing apps specifically. First, the experience indicates that the adoption of data protection legislation remains a critical baseline for the governance of digital technologies. The absence of effective data protection legislation in many states that have introduced apps has accentuated the risks to human rights in both the immediate and long-term. However, data protection legislation alone cannot fully address the risks posed by the use of digital technologies, particularly where they have AI dimensions, and can inadvertently create obstacles to a more comprehensive approach to human rights risks due to the narrowing effects its specificity creates.

Second, the experience of the use of contact tracing apps during the pandemic highlights the need to approach regulation from different vantage points. In the case of contact tracing apps, the risks to human rights were exacerbated both by the lack of regulation of digital technologies within a particular context – in this case, in the fulfilment of states' due diligence obligations during a pandemic – as well as by the lack of dedicated regulation on public sector uses of such technologies. With regards to pandemics, as noted in Part 2, an international pandemics treaty is already being considered by states. Commentators have also proposed standard-setting on a 'rights-based response to epidemics'[117] such as a General Comment by the UN Committee on Economic, Social and Cultural Rights or the UN Human Rights Committee to 'guide the development and reform of laws, policies and practices related to pandemic preparedness',[118] in order to provide greater specificity to the Siracusa Principles as well as to broaden them beyond their current focus on civil and political rights,[119] to also include economic, social and cultural rights.[120] Within both approaches, it will be important to consider

117 Esther Pearson, 'Human Rights-Based Guidelines for the Response to Infectious Disease Epidemics: Righting the Response', (2018) 24 Australian Journal of Human Rights, 201.

118 Nina Sun, 'Applying Siracusa: A Call for a General Comment on Public Health Emergencies', (2020) Health and Human Rights Journal (proposing a general comment by the Human Rights Committee on 'rights restrictions in public health crises' in order to 'guide the development and reform of laws, policies, and practices related to pandemic preparedness').

119 *Ibid.*

120 Leonard Rubenstein and Matthew Decamp, 'Revisiting Restrictions of Rights after COVID-19', (2020) Health and Human Rights Journal, 321; Lisa Forman and Jillian Clare Kohler,

how digital technologies feature within states' due diligence obligations, particularly with regard to AI technologies which can play a potentially important role in modelling epidemics and pandemics, for example by identification of hotspots and predictions of spread but potentially at the expense of other human rights, as well as the limitations on their use.[121]

Developing standards on the use of digital technologies, particularly with potentially far-reaching consequences such as some uses of AI, within the fulfilment of states' due diligence obligations during disasters is not without risks, however, particularly given the lack of dedicated standards on their use in the public sector. Moreover, the use of digital technologies during pandemics cannot be abstracted from their broader use in the public sector. This is both because many of the risks that arose with digital technologies during the COVID-19 pandemic bear similarities to other public sector uses of these technologies which are important to consider together to avoid fragmentation[122] and because the use of AI technologies in particular during a pandemic may expand and normalise beyond times of 'crisis'.

Accordingly, the case study of contact tracing apps highlights the need to address regulation of digital technologies more generally within the public sector. Standard-setting in the public sector would provide avenues to address structural questions, such as the vetting and procurement of private sector actors and public-private partnerships,[123] that cut across all public sector use of digital technologies. For example, in the context of the pandemic, a Joint Civil Society Statement issued by over 100 organisations argued for the need for data sharing agreements that contain 'sunset clauses, public oversight and other safeguards by default', including ensuring that 'any intervention is firewalled from other business and commercial interests', as well as proposals for external and independent scrutiny of how private companies are vetted, including on their human rights records and in digital surveillance'.[124]

'Global Health and Human Rights in the Time of COVID-19: Response, Restrictions and Legitimacy', (2020) 19 Journal of Human Rights, 550.

121 Sara (Meg) Davis *et al.*, 'An International Pandemic Treaty Must Centre on Human Rights', The BMJ Opinion (10 May 2021); *Roojin Habibi, Tim Fish Hodgson, Benjamin Mason Meier, Ian Seiderman, and Steven Hoffman*, 'Reshaping Global Health Law in the Wake of COVID-19 to Uphold Human Rights', Health and Human Rights Journal (1 June 2021), recognising this point in relation to the proposed international pandemic treaty.

122 See, Wirtz *et al.* (n 9), arguing against a fragmented approach to AI applications in the public sector.

123 See, for example, AI Now Institute, City of Amsterdam, City of Helsinki, Mozilla Foundation, and Nesta, 'Using Procurement Instruments to Ensure Trustworthy AI'.

124 Joint statement, 'States use of digital surveillance technologies to fight pandemic must respect human rights', <www.amnesty.org>.

However, these proposals are not exclusive to the pandemic and could most effectively be addressed through a holistic approach to digital governance in the public sector that could then feed into specific use cases and contexts, such as during pandemics or disasters.

While a dual approach to standard-setting risks overlap and inconsistency, it is also necessary to ensure that consideration of digital technologies is embedded in the two intersecting contexts in which they may be introduced, particularly to mitigate the risks of technosolutionism in due diligence measures, and mission creep into the public sector more broadly, as discussed above, given the fluidity of crises which are not confined to one moment in time.[125]

The use of contact tracing apps during the COVID-19 pandemic also highlights two baseline process-based regulatory priorities which if adopted, would open wider routes for scrutiny and challenge of digital technologies in the public sector, including in times of pandemic, prior to, and during, roll-out. These two priorities are first, a process of meaningful transparency prior to roll-out, and second oversight and review of public sector use of digital technologies. I argue that such a process should cut across the public sector, but should also be embedded in any standards developed for global health pandemics or disasters, to avoid exceptionalism.

I do not raise these two priorities to the exclusion of a wider and more comprehensive accountability system designed to prevent human rights violations and other forms of social harm before they occur and adequate and effectively redress them where they take place. In other writing with Daragh Murray and Vivian Ng, I have argued for the application of the international human rights law framework to algorithmic systems, showing how an accountability system based on prevention, monitoring, oversight, and remedies can map on to the full lifecycle of algorithms (and by implication other forms of AI) through the stages of conceptualisation, design, development and deployment.[126] This system includes the use of tools such as human rights impact assessments to predict and identify human rights harm.[127]

However, within the space of this article, I highlight two aspects of this broader accountability system that I consider require prioritisation and can be undertaken ahead of any more far-reaching legislation on digital technologies,

125 Helene Lambert, Michele Foster and Jane McAdam, 'Refugee Protection in the Covid-19 Crisis and Beyond: The Capacity and Limits of International Law', (2021) 44 University New South Wales Law Journal, 120 (noting that, '[c]rises are not just one-off events but can encompass slower processes of change or deterioration as well').

126 McGregor (n 9).

127 *Ibid.*

particularly focused on AI, such as the proposed EU AI Act, which may still take some time to finalise and bring into force, and is in any case geographically limited in scope. As Federica Lucivero *et al.* argue, transparency is a 'means to accountability'.[128] By leveraging different forms of scrutiny, including parliamentary, judicial, and public,[129] this proposal engages existing regulatory mechanisms which themselves may further articulate how existing standards apply to the use of digital technologies in the public sector, including during pandemics, as well as foregrounding the enactment of dedicated legislation on digital technologies or the establishment of new regulatory functions and bodies.

4.1 *Establishing a Process of Meaningful Transparency and Scrutiny of AI Technologies*

One of the key challenges highlighted by the COVID-19 pandemic was the lack of a process to critically assess the proposed introduction of digital technologies, including those with AI components, or the potential to drive existing and new AI systems, ahead of time.[130] Underpinning these challenges is the ongoing failure to embed core rule of law principles, such as transparency, in the governance of AI technologies in the public sector.

Some national AI strategies already refer to transparency as a key legal or ethical principle but typically do not explain what it means.[131] Other proposals have been made for attention to transparency, for example, the UN Special Rapporteur on Privacy established a taskforce on Privacy and the Protection of Health-Data which issued a recommendation on the development of a right to transparency in the processing of health-related data.[132]

128 Federica Lucivero, Nina Hallowell, Stephanie Johnson, Barbara Prainsack, Gabrielle Samuel and Tamar Sharon, 'COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale', (2020) 17 Journal of Bioethical Inquiry. See also, Heike Felzmann, Eduard Fosch-Villaronga, Christoph Lutz and Aurelia Tamò-Larrieux, 'Towards Transparency by Design for Artificial Intelligence', (2020) 26 Science and Engineering Ethics.

129 Aaron Rieke, Miranda Bogen and David Robinson, 'Public Scrutiny of Automated Decisions: Early Lessons and Emerging Trends', Upturn and Omidyar Network Report (no date) 30 (noting that, '[t]he field needs new ways to obtain knowledge and evidence about how automated systems work in practice, and the domain expertise to wrestle with the difficult normative questions that often lurk just behind the code').

130 Luciano Floridi, 'Mind the App – Considerations on the Ethical Risks of COVID-19 Apps', (2020) Philosophy & Technology, 171.

131 Anna Jobin, Marcello Ienca, and Effy Vayena, 'The Global Landscape of AI Ethics Guidelines', Nature Machine Intelligence (2019).

132 UN General Assembly, 'Report of the Special Rapporteur on the right to privacy on the protection and use of Health-related data' (2019) UN Doc A/74/277, para. 10.

The Toronto Declaration also provides for transparency in 'public sector use of machine learning systems', setting out that transparency and accountability require 'explainability and intelligibility in the use of these technologies so that the impact on affected individuals and groups can be effectively scrutinised by independent entities, responsibilities established, and actors held to account'.[133] To achieve transparency and accountability, the Declaration requires public disclosure of 'where machine learning systems are used in the public sector', including disclosure of 'actions take to identify, document and mitigate against discriminatory or other rights-harming impacts' and the adoption of systems that can be independently audited, rather than 'black box systems'.[134] Article 13 of the draft EU AI Act references transparency for high-risk AI systems and Article 52 also focuses on transparency to the users of 'certain AI systems', for example, where the system is 'intended to interact with natural persons'. However, it does not advance an overall principle on transparency in the public sector. Many governments already use digital technologies, including AI, but they do not typically publish a full audit of technologies in use. This has led to calls from civil society groups for public registers and audits.[135] The production of a register or audit of existing uses of digital technologies in the public sector would offer an important correction to the opacity surrounding current use cases. However, since it can be difficult to roll-back technologies once already in use, transparency on proposed uses of technology would allow for parliamentary and public scrutiny, prior to introduction. Principles on transparency typically focus on current, rather than prospective, use. As discussed in this article, publication of the current or proposed use of a technology needs to specify the context or system in which they are to be used, as well as to highlight potential connections to other systems or downstream uses. For example, as discussed in this article, depending on how defined or classified, contact tracing apps could be described as purely digital or as AI depending on whether the data was already, or could be, used by state or non-state actors for analysis through machine learning.

As illustrated in Part 3, transparency cannot be confined to plans to use a particular technological approach, such as a contact tracing app. Rather, details are required on the particular technological model and how it works 'before and during operation', as a lack of clarity can undermine trust and

133 Toronto Declaration (n 58) para. 32.

134 *Ibid.*

135 Joanna Redden, Lina Dencik & Harry Warne, 'Datafied child welfare services: unpacking politics, economics and power', Policy Studies (2020), noting that '[t]here are no public lists of where and how governments are making use of algorithmic systems for public services, although there have been calls for such a list'.

limit public engagement and scrutiny.[136] However, these details will not be sufficient.[137] For example, the Social Science Research Council argued that even where the Australian Government released the source code of its contact tracing app, 'it has not released the server-side source code, which determines how app-generated data is processed, or the algorithm that winnows Bluetooth-generated contact data into "proximity data" that is legible to contact tracers'.[138] It also argued that transparency cannot be viewed as purely technical but must 'also [involve] clear policies and accountable governance that can instil trust'.[139] In this regard, very little information typically exists on the location of digital technologies within wider strategies for the delivery of public sector mandates or the 'larger political implications of the data systems introduced and their economic underpinnings', making visibility of the wider drivers, need and shifts brought about by the introduction of technologies difficult to see, understand and therefore engage with.[140] The publication of impact assessments reflects a critical tool to identify any human rights concerns and the mitigation strategies proposed ahead of time and to enable further public engagement, scrutiny and debate. As discussed in Part 3, if conducted with sufficient detail, data protection impact assessments can make important contributions to preventing human rights harm since, at least under the GDPR, they are required to examine the impact on fundamental human rights. However, as set out in Part 2, they only focus on one dimension to the use of digital technologies, including AI. For this reason, human rights impact assessments are increasingly proposed as a complement to DPIAs in order to capture the full technological system, including the context in which a system is placed.

Accordingly, enabling meaningful engagement and scrutiny of proposed technologies requires substantial levels of detail on the part of the state including publication of details of the specific technology to be used, including current or future AI connections; an explanation of the problem it is intended

136 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, Joint Statement on Digital Contact Tracing (28 April 2020) 4 and 7, available at <https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7>.

137 Moreover, significant challenges and constraints can arise with technological transparency. See discussion in Heike Felzmann, Eduard Fosch-Villaronga, Christoph Lutz and Aurelia Tamò-Larrieux, 'Towards Transparency by Design for Artificial Intelligence', (2020) 26 Science and Engineering Ethics.

138 Social Science Research Council, Surveillance and the 'New Normal' of Covid-19: Public Health, Data, and Justice (2021).

139 *Ibid.*, 19.

140 Redden *et al.*, (n 135).

to address; the precise reasons for proposing its introduction moving beyond the broad justifications often referenced, for example, as a cost-saving measure or a way to continue to deliver services, where human capacity has been reduced due to cut backs,[141] to increase organisational and task efficiency[142] or as a way of 'bolstering evidence-based decision making';[143] the alternatives (technological and non-technological) considered; the proposed approach to purpose limitation; how it fits within the wider mandate of a public sector agency; and the vetting and proposed involvement of private sector actors. This should be accompanied by a more developed approach to the identification and proposed mitigation of risk, both ensuring that data protection impact assessments fully address the risks entailed in data processing but also addressing the risks beyond data processing, through human rights impact assessments able to examine AI technologies in the round, including in the context in which they are deployed.[144]

Such transparency would provide a concrete process and route to interrogate the necessity and proportionality of an AI technology ahead of time. This would then provide space for assessments of whether dedicated legislation is required to regulate the technology as well as for advocacy campaigns and litigation, all of which would have the potential to either prevent the introduction of the technology where the risks are deemed too high, or to ensure the introduction of safeguards. It would also contribute to addressing current democratic deficits in the use of AI technologies where they are often "done" to communities, as well as facilitating assessments of how the technology may impact groups differently.[145]

141 AI Now Institute, 'Litigating Algorithms: Challenging Government Use of Algorithmic Decision Systems' (2018) 7; Wirtz *et al.* (n 9).

142 David Leslie *et al.*, 'Ethics Review of Machine Learning in Children's Social Care – What Works for Children's Social Care', The Alan Turing Institute, the Rees Centre, University of Oxford (2020).

143 *Ibid.*

144 Mark Latonero and Aaina Agarwal, 'Human Rights Impact Assessments for AI: Learning from Facebook's Failure in Myanmar', Carr Centre Discussion Paper Series (March 2021).

145 Joseph Turow, Michael Hennessy and Nora Draper, 'The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation' (2015) (cited by Linnet Taylor, 'What is Data Justice?', Big Data & Society (2017), observing that, 'the resignation of consumers that companies will collect and use their personal data. They explain that '[r]esignation occurs when a person believes an undesirable outcome is inevitable and feels powerless to stop it'). See also, Jess Whittlestone *et al.*, Ethical and Societal Implications of Algorithms, Data and Artificial Intelligence: A Roadmap for Research (2019) 20.

4.2 *Oversight and Review*

A critical part of determining whether digital technologies can be introduced is also the oversight that accompanies their operation.[146] In this regard, a priority for the public sector is the development of robust internal and independent oversight processes that are able to effectively monitor the implementation of digital technologies in practice.[147] Reflecting on contact-tracing apps, Federica Lucivero *et al.* argue that the membership of such oversight bodies should include user and civil society groups.[148]As discussed during the COVID-19 pandemic, arguments were made for the use of sunset clauses given that it is not always possible to fully predict how human rights will be affected prior to the introduction of such technologies. Sunset clauses would mean that the legal basis for the use of the digital technology would terminate at a specified point in time and require application for renewal.[149] The benefit of this approach is that it would build-in a point for review of how the technology is operating in practice and its impact on human rights and the decision-making process and service-delivery of a public sector body. This is particularly critical for 'experimental technologies' such as contact tracing apps.[150] Requiring a review would also provide a further point for a participatory process and consultation on how the technology works in practice, whether initial justifications for its use still stand, and the adequacy and effectiveness of safeguards in place.[151] This is a point made by Mulligan and Bamberger who point out that an iterative process is needed, 'whereby technologies are invented and then redesigned based on user interactions, which then are reintroduced to users, further interactions occur, and further redesigns implemented'.[152] They thus highlight the

146 Joint Statement (n 136) 430.

147 See, Kate Crawford and Jason Schulz, 'AI Systems as State Actors', (2019) 119 Columbia Law Review, 1944 (identifying the 'lack of clear public accountability and oversight processes' as one of the 'main challenges to public scrutiny of AI').

148 Federica Lucivero *et al.* (n 128).

149 Butenko, (n 114).

150 Federica Lucivero *et al.* (n 128).

151 Urs Gasser, Marcello Ienca, James Scheibner, Joanna Sleigh, Effy Vayena, Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid, (2020) 2 Lancet Digital Health, 431 (advocating 'real time feedback mechanisms').

152 Deirdre Mulligan and Kenneth Bamberger, 'Saving Governance-By-Design', (2018) California Law Review, 743–4 (citing Batya Friedman and Alan Borning, 'Value Sensitive Design as a Pattern: Examples from Informed Consent in Web Browsers and from Urban Simulation', Proceedings of the Directors and Implications of Advanced Computing Symposium 109 (2002)).

importance of avoiding static regulation that is incapable of adjusting once the digital application is deployed and the effects of its deployment clear.[153]

Accordingly, while wider than the context of disasters, the use of digital technologies during the COVID-19 pandemic highlights the importance of the introduction of processes for the consideration of digital technologies in the public sector, prior to their introduction and for ongoing oversight and review, if introduced. Had these processes been in place prior to the COVID-19 pandemic, some of the direct human rights concerns arising from the use of contact tracing apps could have been mitigated as well as the risks of digital technologies diverting resources and attention away from wider public health plans and presenting opportunities for mission-creep.

5 Conclusion

This article has sought to demonstrate the complexities involved in regulating digital, including AI, technologies. As discussed through the case-study of contact tracing apps, individual digital technologies are not hermetically sealed but decisions of whether and how to use them have broader implications, in this case, both in how states develop broader due diligence strategies to prevent and mitigate harm, and in their potential to expand and normalise digital technologies, including surveillance and AI technologies, in the public sector, thus potentially contributing to governance by technology. That the employment of one digital technology can penetrate and shape state policies and strategies in different areas and result in diffuse human rights impacts, highlights that they cannot simply be considered from a sectoral perspective, such as within a global health pandemic, or from a technological perspective alone. Rather, multiple regulatory lenses are required.

This article highlights that the use of digital technologies during the global health pandemic suffered from dual deficiencies in understanding the role of digital technologies within states' due diligence obligations and in the lack of dedicated regulation of digital or AI technologies in the public sector. It has therefore argued for a greater focus on the use of digital technologies in both regulatory contexts in order to avoid the possibility of the introduction of digital technologies within global pandemics with the potential to cause immediate and long-term human rights harm, within and outside of pandemics.

While noting calls for new international standard-setting on human rights and global health pandemics, I argue that such standards need to sit alongside

153 *Ibid.*, 744.

standards covering public sector use of digital technologies to ensure complementarity and avoid some of the inconsistencies and disjuncture between the three sets of due diligence obligations discussed in Part 2. While acknowledging the complexity and uncertainty involved in the regulation of digital technologies, at a minimum, I suggest that the use of digital technologies during the COVID-19 pandemic points to the need for states to establish clear processes for public deliberation and scrutiny of proposed uses of digital technologies in the public sector, particularly where they have an existing or potential AI component or use, built around meaningful transparency. Such processes would not only enable parliamentary scrutiny, but also wider advocacy and litigation prior to roll-out and would offer a further way in which to articulate how existing standards, such as the Siracusa Principles, apply to the use of digital technologies in the public sector.