SHRC
Scottish
Human Rights
Commission

Submission to Scottish Government on Consultation on the Digital Strategy for Scotland

23 December 2020

The Scottish Human Rights Commission was established by the Scottish Commission for Human Rights Act 2006, and formed in 2008. The Commission is the National Human Rights Institution for Scotland and is independent of the Scottish Government and Parliament in the exercise of its functions. The Commission has a general duty to promote human rights and a series of specific powers to protect human rights for everyone in Scotland.

www.scottishhumanrights.com

Contents

Foreword

Digital technology raises important human rights challenges and ethical questions about the kind of society Scotland aspires to be. These include concerns about personal privacy and digital security, the ways in which the facts can become distorted through social media, the ways in which governments work with and regulate the tech industry, and the way that social rights services and goods are provided.

A Digital Strategy for Scotland needs to place human rights at its core, ensuring that the full range of civil, political, economic, social, and cultural rights are guaranteed and protected in all of the government's decisions and policies.

The Commission has commissioned Professor Lorna McGregor and Sabrina Rau of the Human Rights, Big Data and Technology Project (HRBDT) based at the University of Essex, to draft a report that explores the full range of human rights considerations that the Government must take into account for its Digital Strategy.

The report first discusses the range of technologies that may fall under the heading of 'digital technologies', as an umbrella term to refer to a wide range of discrete technologies such as computers, tablets and smart phones and the internet.

Second, the report sets out the potential ways in which digital technologies can advance human rights and contribute to the realisation of the Sustainable Development Goals and recommends that states and businesses commit to innovation with such goals in mind. However, it notes that these goals cannot be achieved unless digital divides are overcome.

Third, the report highlights the range of challenges presented to the enjoyment of human rights, as well as where technologies offer opportunities to advance human rights. These challenges not only relate to core risks to the right to privacy and the prohibition of discrimination. Rather, depending on the purpose and context in which digital technologies are employed, any human right can be put at risk.

Fourth, the report sets out that these risks can be prevented from materialising and mitigated where they occur, through the adoption of a human rights based approach to the design, development and deployment of digital technologies, as exemplified by the PANEL principles. It provides an overview of the approach adopted by other states in their articulation of national digital or 'artificial intelligence' (AI) strategies, identifying best practices, as well as ways in which the Scottish Government, in its updated strategy can surpass these strategies, to become an international model of best practice.

The report ends with a set of recommendations for consideration in the updating of the Digital Strategy. Overall, the report recommends that the Scottish Government must position the protection, and realisation, of all human rights as a core principle and vision for the role of digital technologies in society. For this, it must underscore compliance with the law, including human rights law, as a key principle to ensure the protection of human rights and to prevent human rights trade-offs, and unlawful or arbitrary applications of digital technologies, particularly in key areas of life.

We are grateful to Professor Lorna McGregor and Sabrina Rau for their work on this report, which is included in full below. We hope that this analysis will both inform and orientate thinking on how the development, deployment and oversight of digital technologies must align with a vision of rights respecting, fairer Scotland.

Judith Robertson
Chair, Scottish Human Rights Commission

1. Introduction

1. The Covid-19 pandemic has underscored the critical role digital technologies, such as social media and videoconferencing platforms, play in maintaining connections with our friends, families, and communities.[1] They have been vital in opening spaces for marginalised and discriminated against groups to connect, advancing freedom of association and expression.[2] Digital technologies can facilitate access to information and life-long learning,[3] and in times of disruption, can make continued education possible.[4] They have not only enabled many people to continue working during the Covid-19 pandemic, but have also disrupted resistance to remote and flexible models of working. In doing so, they may 'address barriers to inclusion' in the workforce in the future, for example, for people with caring responsibilities, people with disabilities and people living outside of main towns and cities.[5]

2. Significant emphasis has also been placed on the role of digital technologies in realising many of the UN Sustainable Development Goals (SDGs), for example, SDG 1 (no poverty), 2 (zero hunger), 3 (good health and well-being), 4 (quality education), 6 (clean water and sanitation), 7 (affordable and clean energy) and 11 (sustainable cities).[6] The European Commission's White Paper on Artificial Intelligence also highlights the potential for digital technologies to,

'change our lives by improving healthcare (e.g. making diagnosis more precise, enabling better prevention of diseases), increasing the efficiency of farming, contributing to climate change mitigation and adaptation, improving the efficiency of production systems through predictive maintenance, increasing the security of Europeans, and in many other ways that we can only begin to imagine'.[7]

3. While digital technologies may play a central role in advancing human rights and addressing major societal problems, including in times of disruption, their potential has not yet been fully realised or shared equally within, or between, states. These digital divides increase the possibility that technologies may widen, rather than contribute to, addressing inequalities in society. For example, in a

study of the role of digital technologies in advancing the SDGs, Vinuesa et al found that, while 'AI may act as an enabler for all the targets by providing food, health, water and energy services … it may also trigger inequalities which may act as inhibitors to SDGs 1, 4 and 5'.[8] They also found that these technologies may further concentrate wealth in the Global North 'due to the unevenly distributed educational and computing resources throughout the world' and within societies may widen inequalities by disproportionately benefiting 'those already well-off and educated'.[9] Indeed, the Covid-19 pandemic has underscored the impact the ongoing digital divide in all societies has had on access to education, health services, information, and even food.[10]

4. Moreover, the design, development and deployment of digital technologies present significant risks to human rights. Across all digital technologies, risks to the rights to privacy and non-discrimination arise. Just as access to digital technologies may enhance access to information, it may also narrow and distort it through targeting users with media based on their inferred interests and preferences which can inhibit access to a plurality of news alongside increasing levels of disinformation spread online.[11] Further threats to human rights can result from the context in which the digital technologies are used or the reason for their deployment in both the public and private sector. In this regard, all human rights – from the right to education, to the right an adequate standard of living, to freedom of movement, to freedom of association, to the right to liberty - can be put at risk. The rights of access to justice and to an adequate and effective remedy can also prove challenging to exercise, adding a further human rights dimension to the use of digital technologies.[12]

5. The regulation and governance of the design, development and deployment of digital technologies is therefore critical not only to create the conditions for innovation but also to ensure that digital technologies are used to advance, rather than put at risk, equality and human rights. As the UN Secretary General has underscored, '[w]e have a collective responsibility to give direction to these

technologies so that we maximize benefits and curtail unintended consequences and malicious use'.[13]

6. Digital strategies, such as the strategy currently being updated by the Scottish Government, are a key part of a wider and multi-layered governance framework. Such strategies cannot enter into granular detail on how each technology in a particular context should be regulated and governed. However, they are critical to setting out a vision for the role of digital technologies in society and in confirming the key legal and ethical principles that should underpin the design, development and deployment of digital technologies. They provide important guidance to actors in the public and private sector and can foreground more detailed regulation. The Scottish Government's Digital Strategy already places fairness and inclusivity at the heart of its vision.[14] The update of this Strategy provides an opportunity to build on this vision both by recognising the protection and advancement of human rights as a core principle but also in setting out in more detail the key principles, frameworks and processes by which this can be achieved. Such an approach would not only further strengthen the protection of human rights in Scotland but also provide a model digital strategy that can be followed by the many other cities, regions, and states currently developing digital strategies.

2. An Overview of Digital Technologies

7. In this report, we use 'digital technologies' as an umbrella term to refer to a wide range of discrete technologies. These technologies include digital infrastructure and internet-enabled devices, such as computers, tablets and smart phones for personal, business and public use as well as the internet of things which is a 'network of billions of interconnected devices or systems that can be remotely controlled over the internet'.[15] They may also include the digitisation of physical records, such as court or health records, or online portals for accessing information, such as the mygov.scots portal in Scotland which acts as a central point for accessing public services and information.[16]

8. Digital technologies can also refer to processes that are fully or partly automated and to technologies often referred to under the umbrella term of 'artificial intelligence' (AI) technologies. While there is no universal definition of AI, the European Commission uses the following definition:

> Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).[17]

9. Vast amounts of data are required to train and develop most digital technologies, which themselves generate data that often feed into, and enable, other digital technologies. Accordingly, data analytics and data processing form a central part of the digital technology ecosystem. Under the General Data Protection Regulation (GDPR) that came into force in May 2018, data processing refers to,

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated

means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[18]

10. Within the public and private sector, machine learning algorithms are increasingly used to allocate risk and to make predictions and inferences about people and their future behaviour, including to detect fraud; rank news stories; assist in employment decisions; support decisions on migration, welfare, and social security decisions; protect children at risk; and in law enforcement operations.[19] Such automation can also be carried out in combination with other technologies, such as the widely reported trialling of facial recognition technologies by different police forces in the UK and elsewhere.[20]

11. As discussed throughout this report, the wide range of technologies, their functionality, the purpose and context in which they are used, and their consequent effects, present challenges for governance and regulation. At the same time, as highlighted below, most, if not all, uses of technology present risks to the rights to privacy and non-discrimination, as well as other human rights depending on the purpose and context of use. Ongoing digital divides also exclude many people from the benefits of digital technologies, including as a means to realise their human rights. Accordingly, digital strategies, while covering a broad range of technologies, can still identify core principles to address inequalities and ensure the protection of human rights.

3. Prioritising Innovation for Social Good in Scotland's Digital Strategy and Addressing the Digital Divide

12. As set out in the introduction, digital technologies have already, and hold great further potential, to contribute to the resolution of major societal challenges, and to advance our enjoyment of human rights. For example, The Royal Society of Edinburgh has highlighted a range of benefits to being digitally connected, including 'enhanced education and training opportunities, new routes to jobs, greater flexibility in working practices, improved levels of health, new opportunities to increased social interaction and access to a vast swathe of information and resources'.[21] In this year's National Review of Scotland and the SDGs, the Scottish Government pointed to the role of digital technologies in realising the SDGs, such as digital media facilitating the circulation of practical solutions for farmers to mitigate climate change under the SDG 2 on zero hunger[22]; the Digital Health and Care Strategy as a means to meet SDG 3 on good health and well-being[23]; and the Digital Scotland Business Excellence Partnership to meet SDG 8 on decent work and economic growth[24]. Under SDG 9 on industry, innovation and infrastructure, the Review pointed to figures showing that 'superfast broadband coverage in Scotland has increased from 59.3% in 2014 to 93.4% now' acknowledging that digital infrastructure will 'create greater opportunities for education, work and leisure as well as enabling economic growth – particularly in rural Scotland'.[25]

13. Digital technologies not only play an important role in realising key civil and political rights, such as freedom of expression and assembly, but may also support the delivery of certain economic and social rights. For example, the UN Secretary General states that 'information and communication technology can expand the availability and accessibility of quality health services' and 'artificial intelligence has been used to develop new medicines, provide personalised treatment plans and improve the efficiency of care delivery'.[26]

14. The Covid-19 pandemic has illustrated the centrality of digital technologies to the delivery of the right to the highest attainable standard of health. This has both been in facilitating access to healthcare remotely to avoid virus exposure, building on existing developments in e-health[27], but also the role of '[s]upercomputers [in] analys[ing] thousands of drug compounds to identify candidates for treatments and vaccines [and] E-commerce platforms prioritize household staples and medical supplies'.[28]

15. Digital technologies offer a range of opportunities to enhance the availability, accessibility and quality of education. Global investment in Education technology (EdTech) reached over 14 billion GBP in 2019 with a projection of reaching 263 Billion GBP by 2025.[29] It is through video conferencing, online platforms virtual tutoring, and online learning software that education has been enabled with closures of schools due to Covid-19.[30] In this context child rights can also be realised.[31]

16. Beyond Covid-19, online learning platforms have been used by international organisations such as UNESCO in offering education tools in real time to students in remote areas of Mozambique and Zimbabwe.[32] UNESCO, UNHCR and UNICEF have also undertaken similar initiatives in providing education to refugees through online and offline interactive AI-powered learning platforms.[33] Technologies have also been developed to enhance access to education for persons with disabilities, for example, by converting learning materials into Braille and audio version through AI.[34]

17. As one of the authors to this report (McGregor) highlights in a forthcoming report co-authored with Neil Crowther, digital technologies also hold significant potential to enhance the rights of older people to live autonomous, independent and dignified lives.[35] This is not only in relation to increased connectivity but also through technologies that are able to monitor for falls, issue reminders to take medicines, and support memory.[36] When delivered as part of a rights-based, social model of care these technologies have the potential to support older people to live in their homes and

participate and be included in the community, and potentially move away from large care home models.[37]

18. However, for digital technologies to play a role in realising human rights and the SDGs, states and businesses need to purposefully[38] invest in, and prioritise, the development of digital technologies to play a role in resolving societal challenges, particularly by groups in marginalised positions or who have been subject to discrimination.

19. As discussed further below, the prioritisation of innovation for social good and the advancement of the enjoyment of some human rights, cannot be at the expense of, or by trading off, the enjoyment of other human rights. In the examples above, while digital technologies may advance the enjoyment of particular rights, risks to other human rights can arise. For instance, risks can arise where, through personalised education, data relates to a person's (developing) thoughts, or intimate data through the placement of technologies in a person's home, including in bathrooms and bedrooms. Risks also arise depending on whether data are shared or sold and if inferences are drawn through them. Further issues arise if these technologies are introduced in a framework focused on cost-cutting or enhancing efficiencies rather than within a rights-based approach to education, health and care. In such contexts, the result of digitisation could be lower quality education, health or care, or the reduction in human contact, with the potential for a two-tier system to materialise where some are able to access human-delivered services, using digital technologies to enhance such delivery, and others become subject to digital technologies as a replacement of face-to-face services.[39]

20. Adequate investment in, and effective strategies, to overcome the digital divide will also be central to the realisation of human rights, such as to health, education and care, through digital technologies. Significant digital divides continue to persist worldwide.[40] These can arise from poor digital infrastructure and network coverage, access to physical devices and the internet, the cost of data, and digital literacy. An OECD report highlights a persisting digital divide with '327 million fewer women than men hav[ing] a smartphone and can

access the mobile Internet'.[41] The UN Secretary General High Level Panel on Digital Cooperation also highlighted the impact of digital divides on particular groups, noting that,

> People who lack safe and affordable access to digital technologies are overwhelmingly from groups who are already marginalised: women, elderly people and those with disabilities; indigenous groups; and those who live in poor, remote or rural areas.[42]

21. As already highlighted, the effect of these digital divides has adversely impacted many people and communities in the course of the Covid-19 pandemic, precisely in the areas that digital technologies can offer many benefits, such as access to health care, support from public services, reporting domestic and intimate violence and education.[43] The Guardian newspaper interviewed representatives of a number of charities in the UK on the impact of the digital divide during the pandemic, reporting instances of parents only eating twice a day in order to enable their children to access data for schooling, and the adverse impact of a lack of access to devices and data on 'vulnerable groups such as elderly people, asylum seekers and refugees' as well as victims of domestic violence.[44] The article quoted the Chief Executive of Age UK East London as stating that,

> We had one man last week who hadn't eaten in over a week because he didn't have enough money to make a phone call and didn't know who to go for help. We have elderly people who can't get on council shielding lists because you have to register online. Others have ended up critically ill in hospital who have to beg to use a healthcare workers device just to make contact with their family.[45]

22. In a recent General Comment, the UN Committee on Economic, Social and Cultural Rights provided that, 'States parties should ensure that everyone has equal access to the applications of science, particularly when they are instrumental for the enjoyment of other economic, social and cultural rights'.[46] In a post written earlier in the pandemic, one of the authors to this report (McGregor) and Dr

Ahmed Shaheed, proposed five principles 'as immediate priorities for states in responding to harm caused by the digital divide during the COVID-19 pandemic' as 'first steps towards a multi-layered and multilateral strategy to closing the digital divide', as:

1. 'Guaranteeing Internet Access as a Human Rights and Public Good
2. 'Increasing Availability and Acceptability of Digital Infrastructure
3. 'Increasing Accessibility and Affordability of Digital Services
4. 'Empowering People by Addressing Disinformation and Hate Speech without Censorship
5. 'Enabling Access Online Should Not Be a Cause for More Surveillance'.[47]

23. As set out in Part V, a priority for the Digital Strategy should be a vision for policies and practices capable of immediate implementation to address the digital divide, if digital technologies are to avoid perpetuating discrimination and inequality and enable the realisation of human rights, including economic and social rights.

4. Risks of Digital Technologies to Human Rights

24. As discussed in the previous section, even where digital technologies can support the resolution of societal challenges and the enjoyment of human rights, the way in which they are designed, developed, and deployed can present serious risks to human rights. As highlighted by the Scottish Government's consultation paper, digital technologies can interfere with the right to privacy.[48] They also often raise risks of discrimination, even if unintentional, as well as threaten freedom of opinion and expression. Depending on how they are designed; the purpose and context in which they are used; and the safeguards and oversight systems in place, they can threaten many other human rights. It is therefore critical that where states directly develop or procure digital technologies, and in meeting their due diligence obligations to ensure the protection of human rights by third parties, including businesses, they put in place laws, policies, and practices to effectively protect human rights. This part of the report highlights the risks to human rights and the ways in which they can arise.

4.1 Risks to the Right to Privacy

25. Similar to article 8 of the European Convention on Human Rights, article 17 of the International Covenant on Civil and Political Rights states that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'.[49] As the UN High Commissioner for Human Rights has noted, digital technologies 'threaten to create an intrusive digital environment in which both States and business enterprises are able to conduct surveillance, analyse, predict and even manipulate people's behaviour to an unprecedented degree', and thus put the right to privacy at serious risk.[50]

26. These data are not only generated from our private electronic correspondence or social media posts but also from the use of internet-connected devices (internet of things), and other

surveillance tools, such as facial recognition technologies, as discussed below. In some instances, data may be obtained through a data breach, cyber-attacks or unlawful data sharing. For example, in one of the most widely reported instances of alleged unlawful data sharing, Facebook shared the data of 87 million people with Cambridge Analytica, a data analysis firm. Cambridge Analytica was then reported to have used these data to micro-target voters in the United States during the 2016 US election.[51] In May 2019, Canva, an Australian graphic design tool website, was reported to have been subject to a cyber-attack that resulted in the data of 137 million account users including their email addresses, usernames, names, a cities of residence being compromised.[52] In the UK, the Information Commissioner's Office (ICO) found that Royal Free Hospital had 'failed to comply with the Data Protection Act when it provided personal data of 1.6 million patients to DeepMind, a Google subsidiary'.[53] As it may be impossible to know what will be done with the data once it has been shared or sold, the full impact on the right to privacy – as well as other human rights – may not be known and the harm may be difficult to quantify, particularly as it may continue in the future.[54]

27. In some circumstances, data may be ostensibly collected through consent. While consent is one of the six legal bases for processing data under the GDPR and the means by which data are often collected, issues can arise with whether consent has been meaningfully given.[55] These issues arise in the first instance by how the requests themselves are designed, and whether sufficient information is given to people about what will happen with their data, including access by third parties. Such design decisions in consent requests create a lack of clarity, specificity and accessibility that are needed for a user to make an informed decision about whether to consent, putting a heavy burden on the individual to be their own data manager often with insufficient information to carry out this role. Other challenges such as the privacy paradox and consensual exhaustion present further obstacles to the individual being fully informed and able to freely give consent.[56] Furthermore, the nature and context in which data is collected, processed and

shared often times has unforeseeable consequences where there is a lack of specificity on the purpose of the data processing. Due to the imbalance of power between the individual and data controller, the essential negotiating position to allow for free consent may also be lacking. Even where an individual has meaningfully consented to the use of their own data, it is likely to be entangled with data about other people in their lives, on whose behalf they cannot consent. This raises additional privacy concerns, including to intimate and sensitive data such as health data.[57]

28. Even if a single piece of data is not meaningful in and of itself, the collection and aggregation of personal data as well as metadata (data about other data[58]) from single or multiple sources can provide in depth – albeit incomplete and potentially false or inaccurate – insights into an individual's life. As discussed further below, these insights may be used to make inferences about individuals, as well as predictions about their future behaviour, and may be used by public and private actors to make decisions about them, including key life events, as well as target them with advertisements, political campaigns and disinformation.

29. Infringements to the right to privacy can also result in other human rights being put at risk as a result of how the data are used. As a result, the right to privacy has been referred to as a 'gateway right'[59] as if it is protected, other rights will also be protected; conversely, if it is breached, other rights are also put at risk. For example, the B-Tech Team at the Office for the High Commissioner for Human Rights has noted that,

> Credible reports, including at times from tech companies themselves, reveal cases of large-scale infringements on privacy, exacerbating ethnic conflict and dissemination of hate speech, undermining democratic processes, enhancing state surveillance, putting children at risk, facilitating live-streaming of abhorrent acts like the Christchurch terrorist attack, online violence against women and LGBTI persons and others, and "algorithmic discrimination' (whether in the job market, the criminal justice system or in access to public services).'[60]

4.2 Risks to the Right to Non-Discrimination

30. Article 26 of ICCPR states that '[a]ll persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.'[61] The protection of discrimination is also afforded in article 14 of the European Convention on Human Rights. Discrimination can result from the design, development and deployment of digital technologies. Digital technologies can be harnessed to target individuals and communities and to spread and generate hate and discrimination. For example, the UN Office for the High Commissioner for Human Rights has noted that digital technologies, specifically in the context of communication technologies have 'enabled dangerous and hateful speech against certain racial and religious groups, as well as gender-based discrimination, attacks and violence, including violence against women and girls.'[62] These harms not only take place online but also cause harms offline, putting many other human rights at risk.[63]

31. As discussed further below, digital technologies, particularly if AI-driven, such as machine learning algorithms, are often dependent on data. However, as has been well-documented, these data may be incomplete or contain bias. Such discrimination may then be reproduced and amplified. Discrimination in the way in which digital technologies operate can also result from a lack of diversity in design teams as well as training and testing data on a narrow set of data or the way in which the data are weighed with the result that particular technologies only work accurately for certain people and produce discriminatory outcomes for others.[64] For example, in the UK, Foxglove and the UK Joint Council for the Welfare of Immigrants brought a lawsuit alleging that a 'streaming algorithm' which assigned risk according to nationality in the processing of visa

applications 'entrenched racism and bias into the visa system', with 'a secret list of suspect nationalities automatically given a 'Red' traffic-light risk score' meaning that 'people of these nationalities were likely to be denied a visa'.[65] They also argued that they 'discovered that the algorithm suffered from 'feedback loop' problems known to plague many such automated systems – where past bias and discrimination, fed into a computer program, reinforce future bias and discrimination'. Foxglove reported that the Home Office had settled the case, agreeing to disband the use of the algorithm.[66]

32. As discussed in the next section, facial recognition technologies can perpetuate and amplify discrimination, particularly against ethnic minorities, women and persons with disabilities, as a recent report of the UN High Commissioner for Human Rights notes, 'because it can be used to profile individuals on the basis of their ethnicity, race, national origin, gender and other characteristics' and reaffirmed in a recent report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance.[67]

33. The UN Special Rapporteur on Freedom of Opinion and Expression has also found that, 'AI-driven newsfeeds may also perpetuate and reinforce discriminatory attitudes, while AI profiling and advertising systems have demonstrably facilitated discrimination along racial, religious and gender lines.[68] "Autocomplete" AI functions have also produced racially discriminatory results resulting in litigation over their use.[69]

4.3 Risks to Freedom of Opinion and Expression

34. As well as article 10 of the European Convention on Human Rights, article 19 of the ICCPR provides that, '[e]veryone shall have the right to hold opinions without interference,' and that '[e]veryone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice'.[70] The UN

Human Rights Council has underscored the importance of freedom of expression, noting that it 'is essential for the enjoyment of other human rights and freedoms and constitutes a fundamental pillar for building a democratic society and strengthening democracy'.[71]

35. While digital technologies can advance freedom of expression by providing new ways to communicate and to receive and impart information, their use can also pose serious risks to freedom of expression. For example, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has highlighted the risks posed to freedom of expression depending on how states regulate social media companies and how social media companies moderate content online, finding that,

> International human rights law should be understood as a critical framework for the protection and respect for human rights when combating hateful, offensive, dangerous or disfavoured speech. Online hate speech, the broad category of expression described in the present report, can result in deleterious outcomes. When the phrase is abused, it can provide ill-intentioned States with a tool to punish and restrict speech that is entirely legitimate and even necessary in rights-respecting societies. Some kinds of expression, however, can cause real harm. It can intimidate vulnerable communities into silence, in particular when it involves advocacy of hatred that constitutes incitement to hostility, discrimination or violence. Left unchecked and viral, it can create an environment that undermines public debate and can harm even those who are not users of the subject platform. It is therefore important that States and companies address the problems of hate speech with a determination to protect those at risk of being silenced and to promote open and rigorous debate on even the most sensitive issues in the public interest. [72]

36. The UN Special Rapporteur has further pointed to the risks content moderation can pose to freedom of expression:

> The complexity of decision-making inherent in content moderation may be exacerbated by the introduction of automated processes. Unlike humans, algorithms are today not capable of evaluating cultural context, detecting irony or conducting the critical analysis necessary to accurately identify, for example, "extremist" content or hate speech and are thus more likely to default to content blocking and restriction, undermining the rights of individual users to be heard as well as their right to access information without restriction or censorship.[73]

37. Further risks to freedom of expression can arise from the use of surveillance tools and AI-enabled technologies, including by having a chilling effect on the exercise of freedom of expression and other rights, such as freedom of assembly and association. For example, Pete Fussey and Daragh Murray argue that 'the sense that one is being watched inflicts a chilling effect on a wide range of wholly lawful activity',[74] including 'the ability of individuals to freely access information, to develop their understanding of specific issues, to engage in communication'.[75] The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression further submits that, 'interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression'.[76]

4.4 Further Risks to Human Rights Emanating from the Purpose and Context of Use of Digital Technologies

38. In addition to the core risks to the right to privacy, non-discrimination and freedom of expression, further risks to human rights can arise due to the purpose and context in which the technology is deployed. The following examples, while not exclusive, illustrate such risks.

4.4.1 The Use of Digital Technologies in Law Enforcement

39. Digital technologies are reported to have already been deployed, or are under active consideration, in many areas of law enforcement. For example, the Data Justice Project identifies trends in data driven policing to include 'construction, merging and enhancement of databases, real-time identification and tracking of individuals, predictive policing, analysis of heterogeneous data sets, [and] fighting cybercrime'.[77] These practices can raise many risks to human rights, including the rights to liberty and security, the right to a fair trial, freedom of movement, the right to privacy, freedom of opinion, expression, assembly, and association and the right to non-discrimination. The range of technologies employed also highlights that it is insufficient to assess the human rights impact of discrete technologies in isolation, but they must also be examined in context

and in relation to the overall impact their use has on a particular sector.

40. For example, predictive policing involves the 'use [of] data sets of different sizes to feed into an algorithmic model that is supposed to predict either places where crime is most likely to occur in the near future (place-oriented predictive policing), or persons who are likely to get involved in crime (person-oriented predictive policing)'.[78] Some of the core risks that have been associated with such data-driven policing are data quality, discriminatory capacities, and privacy harms.[79] As already noted, digital technologies, particularly AI-driven technologies, require vast amounts of data. The quality of the data, including the types of biases and data sets that they may contain are reflected in how the technology works. This includes considerations of whether certain data omit part of the population or whether some crime data is incomplete due to underreporting or overreporting due to historic policing practices which may therefore misrepresent crime rates and lead to discriminatory outcomes.[80]

41. The use of these digital technologies can result in harms to many human rights, including the right to liberty and security, freedom of movement, and the right to a fair trial and effective remedy.[81] For example, while the use of these technology may be intended to create more efficiency and save resources, researchers have found that it can lead to over-policing of already heavily policed areas and result in 'disproportionate stop and search practices based on race and ethnicity'[82] as well as impact the right to liberty and security and the right to fair trial.

42. The use of facial recognition technologies in law enforcement, whereby images are checked against databases or watchlists has been subject to widespread critique from a human rights perspective due to the risks its presents to many human rights, such as, privacy, non-discrimination, expression and assembly. For example, a recent report of the UN High Commissioner for Human Rights demonstrated the risks posed by the use of facial recognition technology to the right to peaceful assembly as well as its capacity to reinforce discrimination.[83] Despite noting the advances of facial

recognition technology, the UN High Commissioner for Human Rights points to the error rate in facial recognition technologies, leading to individuals being wrongly flagged leading to detention and prosecution.[84] Particularly discriminated by this technology are 'Afrodescendants and other minorities, women or persons with disabilities'.[85] In a report on predictive policing by Professor Sandu and Professor Fussey they write 'one of the most controversial criticisms of predictive policing is that, in contrast to claims about objectivity made by technology vendors, predictive technology can reinforce bias in police work by creating hotspots which feature an overrepresentation of disadvantaged neighbourhoods with a large population of racial and ethnic minorities as residents… The result is a feedback loop whereby predictive policing outputs refocus policing attention towards marginalised people and places'.[86]

43. Calling for immediate moratorium on the sale, transfer and use of surveillance tools until 'robust human rights safeguards are in place to regulate such practice', the UN Special Rapporteur on Freedom of Opinion and Expression has stated that, '[s]urveillance tools can interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation. And yet they are not subject to any effective global or national control.'[87] He argued that, safeguards should include human rights due diligence, independent oversight strict data protection laws and full transparency of the use of surveillance technology.[88] A range of civil society members, national human rights institutions, academics, and even companies, have also called for a moratorium on the use of facial recognition technologies.[89]

4.4.2 AI and data analytics in education

44. As discussed earlier in this report, digital technologies may contribute to the realisation of the right to education. However, digital technologies may not be fully accessible to all due to various digital divides, or the failure to design technologies with diverse users in mind, including persons with disabilities.

45. Concerns may also arise that reliance on digital technologies to deliver education could lower the quality of education or result in a two-tier situation in which some students receive face-to-face education with digital technologies complementing and extending such education, whereas others experience the replacement of face-to-face teaching with online services. Reflecting on online learning during the Covid-19 pandemic, the UN Special Rapporteur on the Right to Education has stated that such forms of education delivery should be seen as a temporary solution and that 'digitization of education should never replace on-site schooling with teachers'.[90]

46. Under international law states are required to provide resources for the realisation of the right to education including through providing financial support for digital infrastructure, training and taking measures to protect children from online harassment and involvement in illegal activities.[91] A significant concern in relation to the use of digital technologies as a means of delivering the right to education is the role and regulation of businesses providing these platforms and the nature of the agreements they enter into with states. The Special Rapporteur on Education has recognised that 'all providers of education, whether operating independently or jointly with Governments, remain accountable given that States bear responsibility for ensuring respect for the right to education in all partnerships' and that it is of utmost importance that education be safeguarded against the forces of privatisation.[92]

47. The ability of states and private actors to access, collect, analyse and sell data obtained through such platforms has become a serious concern. Human Rights Watch notes that,

> Children's education data are far less protected than health data. Many countries have regulations that govern the appropriate uses and disclosures of personally identifiable health data, even during emergencies. But while children's school data may be just as sensitive – revealing names, home addresses, behaviors, and other highly personal details that can harm children and families when misused – most countries don't have data privacy laws that

protect children. This means that governments will struggle to hold EdTech providers accountable for how they handle children's data.[93]

48. The risks posed to human rights thus raise the state's human rights obligations to ensure the protection of human rights when procuring digital technologies for the delivery of education. The Abidjan Principles on the human rights obligations of States to provide public education and to regulate private involvement in education are a key guidance in this respect.[94] These principles were developed in response to the rapid expansion of private sector involvement in education and compile and interpret existing human rights law and standards in this context. The Abidjan Principles offer guidance on state obligations to 'provide free, public education of the highest attainable quality, regulate private involvement, and fund quality public education'.[95] The Abidjan Principles consist of 97 guiding principles including on the 'obligation to respect, protect and fulfil the right to education to the maximum of available resources'; the 'obligation to respect, protect and fulfil the right to education in the context of private involvement'; 'financial provisions'; 'accountability and monitoring'; and 'implementation and monitoring of the guiding principles'.[96]

4.4.3 Data analytics and AI in social security

49. In 2019, the UN Special Rapporteur on Extreme Poverty and Human Rights emphasised the challenges of digital technologies being used for social protection and security warning that we are 'stumbling, zombielike, into a digital welfare dystopia'.[97]

50. While the opportunities particularly for government to embrace digital systems has grown exponentially and is often justified on the basis of increasing efficiency, in reality such measures are accompanied by 'deep reductions in the overall welfare budget, a narrowing of the beneficiary pool, the elimination of some services, the introduction of demanding and intrusive forms of conditionality, the pursuit of behavioral modification goals, the imposition of stronger sanctions regimes and a complete reversal of the

traditional notion that the State should be accountable to the individual'.[98]

51. Digital technologies are reported to have been used in a wide range of ways for social security in a number of states, including for personal identification, eligibility assessments, welfare benefit calculations and risk scoring. In the UK, the Child Poverty Action Group has found that in the claims process for Universal Credit, 'claimants are not provided with enough information about how their benefit has been calculated, or how to challenge a decision if they believe a mistake has been made'.[99] In the Netherlands, an automated system called SyRI was used to detect the likelihood of individuals committing benefits fraud in economically disadvantaged and high-immigration areas. A court in the Netherlands found that the technology raised excessive privacy concerns with the law providing inadequate safeguards to protect human rights.[100] Similarly, in Sweden an automated decision-making system has been reported to have been used to wrongly deny welfare payments of 70,000 people.[101]

52. In 2018 the Australian government introduced an automate welfare payment suspensions which the Guardian found that '75% of the time, benefits recipients who had their payments suspended under the new system were not at fault'.[102] The errors in such automated systems and the lack of knowledge about such automation and how to challenge them as indicated in the Child Poverty Action Group report risk further entrenching poverty.[103] Similarly, in related to the UK automated benefits system, a Human Rights Watch report notes, '[t]he government's bid to automate the benefits system – no matter the human cost – is pushing people to the brink of poverty.'[104]

53. The digitisation of welfare systems have also created obstacles for access due to ongoing digital divides. For example, Human Rights Watch notes that 'many people that lack digital literacy also cannot afford a computer device or an internet connection' demonstrating not only the digital divide but the challenges in receiving benefits.[105]

4.5 Impact on the Right to an Adequate and Effective Remedy and Access to Justice

54. Where digital technologies impact the enjoyment of people's human rights, obstacles may prevent them from effectively exercising their right to an adequate and effective remedy and to access justice.[106] In some instances, they may not even know that a digital technology has played a role in a decision about them and may therefore be unaware, and unable to challenge, its use. Furthermore, the individual or group experiencing the harm may not be the user of the technology, making the evidence of harm a challenge such as was the case with data of data subjects who did not use the Cambridge Analytica app, but still had their data processed exposing them to potential harm. In other situations, a person may have insufficient information on how the technology, such as an algorithm, works or how it has been used in a decision-making process, making it more challenging to effectively make a complaint. This can often arise where a company will not reveal the source code on grounds of proprietary interest or provide an understandable explanation of how it works and how it has reached particular conclusions. Further questions can arise in relation to standing if a person cannot provide evidence that a technology has been used on them, such as being able to show that facial recognition technology was applied to them during a protest.[107] Moreover, they may face obstacles in proving the nature and level of harm they have suffered.

55. Further issues can arise for complainants in identifying where to make a complaint given unclarity of the range of actors that might also be involved in the development and deployment of the technology. The cost of litigation in many cases will make access to a court prohibitive, unless a complainant can access legal aid. Questions also arise as to the accessibility, availability, affordability, timeliness and effectiveness of other forms of complaints mechanisms within the state, and within companies.

4.6 Conclusion

56. The wide range of contexts in which digital technologies are deployed and the full range of rights that may be implicated as a result of lack of access to technologies, or a lack of safeguards in using or deploying such technologies, demonstrates the importance of multi-layered regulation, including an effective digital strategy. Given the impact on human rights, it is critical that a human rights-based approach sits at the centre of such a digital strategy in order to ensure their effective protection and realisation through digital technologies.

5. Embedding Human Rights Principles in Digital Strategies

57. No dedicated legislation regulating the overall design, development and deployment of digital technologies currently exists. The lack of dedicated legislation does not mean that states are in a regulatory void as they are still required to meet their obligations to protect human rights under national and international law. These obligations arise in two ways. First, as already noted, reports and findings by international organisations, parliaments, national human rights, equality and data protection bodies, media, civil society and academics, and judicial decisions have illustrated the range of ways digital technologies are already being used in the public sector. Such uses raise states' obligations to protect human rights directly. Second, where human rights are put at risk by third party actors, including businesses, states' due diligence obligations under international law arise both generally[108], and pursuant to the specific obligations set out in the UN Guiding Principles on Business and Human Rights in relation to businesses.[109]

58. In the absence of dedicated legislation, digital and AI strategies can play a critical role in translating states' obligations under international human rights law to the digital sphere and can foreground other forms of regulation including legislation. These strategies are necessarily high-level and therefore cannot provide granular direction on the design, development or deployment of individual technologies in specific contexts. Instead, they can identify the key principles and norms by which digital technologies are governed and advance a vision for their place in society. As such, the recognition of the potential impact of digital technologies on human rights, both as a threat and a catalyst to their realisation, as well as key human rights principles relevant to the design, development and deployment of digital technologies is particularly important. In this part of the report, we first set out the key human rights principles relevant to digital strategies before analysing the extent to which these principles are reflected in current digital and AI strategies.[110] We conclude this part of the report by identifying

the ways in which the Scottish Government's updated Strategy can build on these existing strategies.

5.1. Key Human Rights Principles Relevant to the Digital Sphere

59. Digital and AI strategies provide an opportunity and means by which to operationalise human rights. In order to ensure that actors in the digital sphere are clear on their existing obligations and responsibilities to guarantee the effective protection and realisation of human rights, digital strategies need to recognise the obligation to **protect all human rights**, rather than only focus on specific rights, such as the right to privacy, as well as confirm the nature of states' obligations and businesses' responsibilities in this regard. In this section, we provide a short overview of the elements to a human rights-based approach, which are highlighted by the SHRC's PANEL Principles as Participation, Accountability, Non-Discrimination, Equality, Empowerment and Legality.[111]

60. In contrast to many other areas in which human rights are affected, the first critical principle in relation to digital technologies is **transparency**. In this regard, in most states, 'comprehensive information is not available is available on the range of technologies being used, leading to calls for a public register of the use of digital technologies.[112] As noted above, even where the use of a particular technology is known, the reason for its introduction, the details of where and how it is used, and how it works may not be fully known or understood, including when it is used to support individual decision-making in key areas of life. Further, where public sector bodies procure technologies from private actors, the nature of these procurement arrangements are not always made public, or subject to an accountability process, which raises further risks to human rights, particularly where the private sector actor is able to access and/or use data or test a particular technology through the public sector. Clearer mapping of the use of digital technologies across the public sector as well as publishing details of the reasons for its introduction and how it works is important. In addition, direct notification to individuals subject to its use therefore presents a

critical baseline for understanding and assessing the human rights implications of the use of digital technologies in the public sector.

61. Beyond transparency, as illustrated in this report, the rights to privacy, the prohibition of discrimination and freedom of expression are commonly put at risk across a range of technologies. However, depending on the purpose and context in which a technology is used, all other human rights can potentially be put at risk. It is therefore important for digital technologies to **acknowledge the potential for all human rights to be potentially affected**, as well as the ways in which digital technologies can potentially facilitate a range of rights. Without such acknowledgment, where human rights are adversely affected, the seriousness may be understated. Conversely, their potential may go unrealised. It is for this reason that when conducting a human rights impact assessment not only salient, assumed rights should be investigated, but rather impacts on the full range of human rights must be considered.

62. As highlighted by the PANEL Principles, a core principle of a human rights-based approach is the **legality** of the use of digital technologies. This principle not only underscores that the use of digital technologies must have a legal basis but also that they should comply with international human rights law. In this regard, digital technologies can never be used to violate absolute prohibitions under international human rights law. The use of these technologies must also meet tests of necessity and proportionality, which include demonstrating that where there is an interference with rights such as privacy or freedom of expression, that it pursues a legitimate aim and constitutes the least restrictive restriction on the right concerned. In an article with Daragh Murray and Vivian Ng, one of the authors of this report (McGregor) has argued that in certain circumstances, the application of international human rights law may result in a red-line prohibiting the use of the technology. This may arise due to the purpose or effect of the technology on human rights, for example, where it produces discriminatory outcomes, or where insufficient safeguards are in place to protect human rights.[113]

63. **Safeguards** constitute key principles for inclusion and prevention of harm within digital strategies. These include the obligations of states to protect human rights against third party harm and responsibilities of businesses to take adequate and effective measures to prevent the violation of human rights in the first place through the adoption of human rights policies and management systems as well as effective due diligence processes.[114]

64. To ensure **accountability,** appropriate resources and expertise must be dedicated to understanding potential and actual human rights impacts that digital technologies can have. **Impact assessments** offer a practical way for states and businesses to fulfil their obligations and responsibilities under international human rights law, to identify potential risks to human rights, or adverse impact that has already occurred, in order to cease activities causing such harm and prevent it from reoccurring. Impact assessments should be prepared in consultation with key stakeholders and should be undertaken at the conception and design phase of digital technologies; prior to their deployment; and at regular intervals thereafter. Data protection impact assessments as required under the GDPR can support the protection of human rights, although wider human rights impact assessments will be required to ensure all human rights risks are identified, particularly where they do not relate to data processing. Integrating methodologies of human rights impact assessments into data protection impact assessments could also strengthen certain impact assessment practices through better understanding of cumulative impacts, gain further understanding of the conception of risk, increase transparency, provide a means of engaging and empowering stakeholders, and further entrench the need for ongoing review and reporting.[115]

65. As part of the safeguards states and businesses need to put in place, **oversight** processes are critical to identify adverse impacts to human rights and to monitor the deployment of technologies as well as accountability and redress mechanisms where violations occur. These should include internal oversight processes within

public sector agencies and private sector bodies, as well as independent oversight bodies.

66. Accessible, affordable, timely and effective **remedies** are a critical safeguard in the use of digital technologies in the public and private sector. Individuals have a right to access justice and to an effective remedy under international human rights law, both in relation to state use of AI technologies as well as private actors. The third pillar of the UNGPs refers to three categories of grievance mechanisms through which individuals should be able to seek redress.[116] These are state-based-judicial and -non-judicial mechanisms and non-state-based grievance mechanisms. While state based grievance mechanisms form the foundation of a system of remedies, non-state grievance mechanisms should complement such a wider system for impacts to be remediated quickly and directly by companies thereby also preventing future harms.[117]

67. Alongside processes to identify and address risks to human rights, **the right to benefit from scientific progress** reflects a principle well-positioned to focus the design, development and deployment of digital technologies on the realisation of human rights, including by **overcoming digital divides**.

68. Finally, the design, development and deployment of digital technologies alongside governance processes have been heavily critiqued for their lack of diversity and participation. In this regard, the PANEL Principles of **participation and empowerment** are particularly relevant to the digital technology sphere in widening the participation and influence of those involved not only on decisions on the design and whether and how to use specific technologies but also their broader place in society, as well as their regulation and oversight.

5.2 An Overview of the Inclusion of Human Rights Norms in Existing Digital and AI Strategies

69. In digital and AI strategies adopted to date, the principles discussed in the previous section have not been fully adopted although states

increasingly make reference to human rights principles and norms. Surveying national AI strategies as well as strategies produced by businesses and non-governmental organisations, Jobin, Ienca and Vayena argue that there is a 'global convergence emerging around five ethical principles (transparency, justice and fairness, non-maleficence, responsibility and privacy)'[118]. They also point out that most of these strategies have been adopted in the Global North, creating an imbalance in the approach to regulation.[119] In a forthcoming study on the treatment of human rights principles in published national AI strategies, one of the authors of this report (McGregor) and Elena Abrusci identify a number of trends.[120]

70. First, many, although not all, strategies recognise the importance of the protection of human rights (or fundamental rights) in the digital sphere, including as a core guiding principle for the use of AI technologies.[121] In relation to the core rights potentially impacted by the design, development and deployment of AI technologies, many, although not all strategies, refer to the right to privacy[122], and fewer refer to the prohibition of discrimination[123] or freedom of expression[124]. The practice of states is much more varied with regard to recognition of the impact of AI technologies on other human rights, or the contexts in which further rights' concerns might arise. In the national strategies we surveyed, only a few mentioned the impact of AI technologies on health[125], education[126] and work[127], but even where they did, they typically did not refer to human rights, with the exception of one framing of work in terms of rights.[128] Moreover, many other sectors were omitted, such as social care.

71. Second, the practice of states is much more varied with regard to references to particular groups that may be affected by the use of digital technologies. In the national AI strategies we surveyed, some make reference to certain groups, such as women[129], children[130], older people[131], people with disabilities.[132] Other strategies refer more generally to the need to 'support disadvantaged groups […] most at risk due to automation'[133]; ensure that 'artificial intelligence [does] not reproduce prejudices that marginalise specific population groups'[134]; be used to reduce inequalities.[135]Many states make

reference to the importance of transparency, although they vary in the depth and specificity they give to the principle.[136]

72. Third, many states refer to accountability as a core AI principle[137] but very few refer to the importance of access to justice and the right to a remedy. For example, Malta's strategy provides that, 'accessible complaints resolution processes should be implemented to ensure effective redress for individuals harmed by AI systems'.[138] Similarly, very few states refer to the importance of oversight mechanisms and for the role for impact assessments in identifying harm already caused or with the potential to be caused by the use of AI systems. For example, some states refer to the need to monitor the impact of AI technologies[139] and others refer to the establishment of an ethics or oversight body.[140] Some also include the need to carry out impact assessments. For example, Germany's strategy states that an impact assessment 'of these technologies with regards to their implications for the world of work and society as a whole' should be carried out.[141]

73. Fourth, many strategies also refer to the importance of the principles of participation and inclusion[142] with many including them as core principles.

74. Accordingly, while many AI strategies reflect some key human rights principles, none comprehensively adopt a full human rights-based approach. 'These gaps create the risk that the potential of digital technologies to advance human rights, particularly social rights, will not be realised, and that the enjoyment of other human rights will be threatened'.

5.3 Recommendations for Scotland's Updated Digital Strategy in Order to Become a Model of Best Practice

75. The updating of Scotland's Digital Strategy provides a critical opportunity for the Scottish Government to build on, and go beyond, many of the digital and AI strategies already issued, by creating a vision for the role of digital technologies in Scotland that prioritises the design, development and deployment of digital technologies to

advance human rights and the SDGs. Such a vision can ensure that the benefits of digital technologies contribute to a fairer society, contribute to addressing discrimination and inequalities, and strengthen human rights protection.

76. In order to achieve this goal, this report makes 10 key recommendations:

1. Position the protection, and realisation, of all human rights as a core principle and vision for the role of digital technologies in society and employ human rights language to provide a common language to frame harm.

2. Guarantee diverse and meaningful participation, empowerment and inclusion in decisions of whether and how to employ digital technologies and in their oversight.

3. Commit to the adoption of a 'multi-layered and multilateral strategy to closing the digital divides' in Scotland, by guaranteeing internet access as a right and a public good; and increasing 'availability and acceptability of digital infrastructure' and the 'accessibility and affordability of digital services'[143], paying particular attention to digital divides affecting groups in positions of marginalisation.

4. Underscore compliance with the law, including human rights law, as a key principle to ensuring the protection of human rights and to prevent human rights trade-offs, and unlawful or arbitrary applications of digital technologies, particularly in key areas of life.

5. Commit to transparency in the use of digital technologies in the public sector, including where technologies are procured or operated by, or with, the involvement of the private sector.

6. Commit to publishing a public register on where digital technologies are already being used in the public sector and the role of private companies, and going forward, to publish details of digital technologies under consideration in order to empower rights-holders and allow for a full public debate and scrutiny of their desirability, purpose, and potential human rights implications prior to adoption.

7. Carry out a human rights impact assessment prior to the deployment of digital technologies and new relationships/partnerships and at regular intervals and at 'critical gateways'[144] thereafter in the public sector and support the introduction of mandatory due diligence processes for public and private sector actors using digital technologies in Scotland.

8. Introduce monitoring and oversight processes for the use of digital technologies in the public sector where human rights are at risk, and require similar processes within the private sector as per the UNGPs.

9. Ensure that individuals whose human rights are affected by the use of digital technologies whether in the public or private sector are able to access affordable, timely and effective remedies.

10. Where digital technologies are considered in particular sectors, such as health, social care, and education, require dedicated strategies that ensure the realisation and protection of human rights.

[1] Report of the UN Secretary-General's Roadmap for Digital Cooperation, June 2020, p 2, available at https://www.un.org/en/content/digital-cooperation-roadmap/

[2] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348, 29 August 2018, available at https://www.undocs.org/A/73/348
[3] Ibid.
[4] Utkarch Ambitabh, 'How Technology will Transform Learning in the COVID-19 Era', World Economic Forum, 31 August 2020, available at https://www.weforum.org/agenda/2020/08/how-edtech-will-transform-learning-in-the-covid-19-era/
[5] Oliver Wright and Zara Ingilzian, 'COVID-19: It's Time to Rethink Where, How and Why We Work', World Economic Forum, 17 August 2020, available at: www.weforum.org/agenda/2020/08/covid-19-future-of-work-employees/
[6] Celine Herweijer, Domenic Kailash, Nath Waughray, 'How Technology Can Fast-Track the Global Goals', World Economic Forum, 24 Sept 2019, available at https://www.weforum.org/agenda/2019/09/technology-global-goals-sustainable-development-sdgs/
[7] 'White Paper on Artificial Intelligence- A European Approach to Excellence and Trust', European Commission, 19 February 2020, available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf
[8] Vinuesa, Ricardo, Hossein Azizpour, Iolanda Leite, Madeline Balaam, "The Role of Artificial Intelligence in Achieving the Sustainable Development Goals', January 2020, available at https://www.researchgate.net/publication/338554769_The_role_of_artificial_intelligence_in_achieving_the_Sustainable_Development_Goals
[9] Ibid.
[10] John Lai, Nicole O. Widmar, 'Revisiting the Digital Divide in the COVID-19 Era', 3 October 2020, Applied Economic Perspectives and Policy, available at https://onlinelibrary.wiley.com/doi/10.1002/aepp.13104 ; '"Pay the Wi-Fi or Feed the Children": Coronavirus has Intensified the UK's Digital Divide', University of Cambridge, available at https://www.cam.ac.uk/stories/digitaldivide
[11] Nathalie Marachel, Rebecca MacKinnon, Jessica Dheere, 'Targeted Advertising and COVID-19 Misinformation: A Toxic Combination', Ranking Digital Rights, 27 May 2020, available at https://www.newamerica.org/oti/reports/getting-to-the-source-of-infodemics-its-the-business-model/targeted-advertising-and-covid-19-misinformation-a-toxic-combination
[12] 'Expert Meeting on the Technology Sector and Access to Remedy Through Non-State-Based Grievance Mechanisms', Human Rights, Big Data and Technology Project and OHCHR, 11 June 2019, available at https://www.ohchr.org/Documents/Issues/Business/B-Tech/HRBDTOHCHRExpertMeetingTunis6September2019.pdf
[13] UN Secretary-General's 'Roadmap for Digital Cooperation: Implementation of the Recommendations of the High-level Panel on Digital Cooperation', A/74/821, 29 May 2020, Available at https://www.un.org/en/content/digital-cooperation-roadmap/
[14] 'Renewing Scotland's full potential in the digital world: updating the digital strategy for Scotland - discussion document', Scottish Government, September 2020, p 8, available at https://www.gov.scot/publications/renewing-scotlands-full-potential-digital-world/
[15] 'Internet of Things', European Commission, 18 September 2019, available at https://ec.europa.eu/digital-single-market/en/news/internet-things-brochure
[16]'Access to Public Services in Scotland', mygov.scot, available at https://www.mygov.scot/
[17] 'A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines', European Commission, 8 April 2019, available at https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines
[18] European Parliament and Council of European Union (2016) *Regulation (EU) 2016/679*, Art 4 (2), 27 April 2016, Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

[19] 'Public Scrutiny of Automated Decisions: Early Lessons and Emerging Methods', Upturn and Omidyar Network Report, 27 February 2018, available at https://omidyar.com/public-scrutiny-of-automated-decisions-early-lessons-and-emerging-methods/

[20] Pete Fussey, Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology', Human Rights, Big Data and Technology Project, 3 July 2019, available at https://www.hrbdt.ac.uk/publications/
[21] Douglas White, 'Digital Participation and Social Justice in Scotland' , Carnegie UK, September 2016, p 4, available at https://d1ssu070pg2v9i.cloudfront.net/pex/carnegie_uk_trust/2016/09/v3-2697-CUKT-Digital-Participation-summary.pdf
[22]'Scotland and the Sustainable Development Goals - A National Review to Drive Action', SDG Network Scotland and The Scottish Government, July 2020, p 28, available at https://globalgoals.scot/scottish-sdgs-national-review-2020/,
[23] Ibid. p 40
[24] Ibid. p 113
[25] Ibid p 125; 'Superfast Broadband', Digital Scotland, available at https://www.scotlandsuperfast.com/
[26] Report of the Secretary General on the 'Question of the Realization of Economic, Social and Cultural Rights in All Countries: The Role of Technologies for the Realization of Economic, Social and Cultural Rights', 4 March 2020, A/HRC/43/29, para 19- 20, available at https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf
[27] 'E-health Good Practice Case Studies', The Scottish Government and NHS Scotland, available at https://www.ehealth.scot/
[28] UN Secretary-General's Roadmap for Digital Cooperation: Implementation of the Recommendations of the High-Level Panel on Digital Cooperation', A/74/821, 29 May 2020, p 4, Available at https://www.un.org/en/content/digital-cooperation-roadmap/,

[29] 'The COVID-19 Pandemic has Changed Education Forever. This is How' World Economic Forum, 29 April 2020, https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/

[30] Ibid.

[31] 'Generation AI: Engaging Stakeholders to Build AI Powered Solutions that Help Realize and Uphold Child Rights', UNICEF, available at https://www.unicef.org/innovation/GenerationAI ; Erica Kochi, Jennie Bernstein, Tushar Ghei, 'How can UNICEF, the World economic Forum and Others Work Together to Advance Children's Rights in the AI Age? Reflection from Our Generation AI Workshop', UNICEF, 10 December 2018, available at https://www.unicef.org/innovation/stories/generation-ai

[32] Lorna McGregor, Vivian Ng and Ahmed Shaheed, 'The Universal Declaration of Human Rights at 70: Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence', Human Rights Big Data and Technology Project, 20 December 2018, p 17, available at https://www.hrbdt.ac.uk/the-universal-declaration-of-human-rights-at-70-putting-human-rights-at-the-heart-of-the-design-development-and-deployment-of-artificial-intelligence/ ; See also 'ICT Transforming Education in Africa Project', UNESCO, available at https://en.unesco.org/themes/ict-education/kfit <http://unesdoc.unesco.org/images/0026/002659/265908E.pdf>.

[33] Lorna McGregor, Vivian Ng and Ahmed Shaheed, 'The Universal Declaration of Human Rights at 70: Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence', Human Rights Big Data and Technology Project, 20 December 2018, p 17, available at https://www.hrbdt.ac.uk/the-universal-declaration-of-human-rights-at-70-putting-human-rights-at-the-heart-of-the-design-development-and-deployment-of-artificial-intelligence/ ; 'A Lifeline to Learning: Leveraging Technology to Support Education for Refugees', UNESCO, Paris 2018, available at http://unesdoc.unesco.org/images/0026/002612/261278e.pdf ; See also, the Global Compact on Refugees, Report of the United Nations High Commissioner for Refugees, 'Part II Global Compact on Refugees', A/73/12 (Part II), 13 September 2018, available at https://www.unhcr.org/gcr/GCR_English.pdf

[34] See 'Artificial Intelligence in the Classroom' (*Microsoft Education*, 1 March 2018), available at https://educationblog.microsoft.com/2018/03/artificial-intelligence-in-the-classroom/ and 'Microsoft Translator for Education', available at https://translator.microsoft.com/help/education/

[35] Neil Crowther and Lorna McGregor, 'A Digital Cage is Still a Cage: Designing and Deploying AI Technologies in Social Care to Advance – Not Violate Older People's Human Rights' forthcoming 2021.*See also,* Scottish Care, TechRights: Human Rights, Technology and Social Care, 2018 available at: https://scottishcare.org/wp-content/uploads/2019/11/TechRights-Human-Rights-Technology-and-Social-Care.pdf
[36] Crowther and McGregor ibid.
[37] Ibid. *See also,* 'Human Rights Charter for Technology and Digital and Digital in Social Care Guidance Document', Scottish Care, September 2019, available at https://scottishcare.org/wp-content/uploads/2019/11/Guidance-Document-for-Human-Rights-Charter-for-Technology-Digital-in-Social-Care.pdf
[38] Report of the UN Secretary-General's High-level Panel on Digital Cooperation, p 6, A/74/821, 29 May 2020, p 7, available at https://www.un.org/en/content/digital-cooperation-roadmap/,
[39] Lorna McGregor, Vivian Ng and Ahmed Shaheed, 'The Universal Declaration of Human Rights at 70: Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence, Human Rights Big Data and Technology Project, 20 December 2018, p 17, available at https://www.hrbdt.ac.uk/the-universal-declaration-of-human-rights-at-70-putting-human-rights-at-the-heart-of-the-design-development-and-deployment-of-artificial-intelligence/
[40] Fara Zahri, 'Digital Divide' Will Worsen Inequalities, Without Better Global Cooperation', UN News, 4 September 2019, available at https://news.un.org/en/story/2019/09/1045572
[41] 'Bridging the Digital Gender Divide: Include, Upskill, Innovate', OECD, 2018, available at www.oecd.org/digital/bridging-the-digital-gender-divide.pdf
[42] 'The Impact of Covid-19 on Older Persons', United Nations, May 2020, available at 6; un_policy_brief_on_covid-19_and_older_persons_1_may_2020.pdf
[43] 'Digital Divide "a Matter of Life and Death" amid COVID-19 Crisis, Secretary-General Warns Virtual Meeting, Stressing Universal Connectivity Key for Health, Development', UN Secretary General, 11 June 2020, available at https://www.un.org/press/en/2020/sgsm20118.doc.htm
[44] Annie Kelly, 'Digital Divide "Isolates and Endangers" Millions of UK's Poorest', The Guardian, 28 April 2020, available at https://www.theguardian.com/world/2020/apr/28/digital-divide-isolates-and-endangers-millions-of-uk-poorest
[45] Ibid.
[46]General comment No. 25 (2020) on Science and Economic, Social and Cultural Rights (article 15 (1) (b), (2), (3) and (4) of the International Covenant on Economic, Social and Cultural Rights), para 17, available at https://undocs.org/E/C.12/GC/25
[47] Lorna McGregor and Ahmed Shaheed, 'The COVID-19 Pandemic: Five Urgent Principles for Leaving No One Behind Through Technology', 19 May 2020, available at https://www.universal-rights.org/blog/the-covid-19-pandemic-five-urgent-principles-for-leaving-no-one-behind-through-technology/
[48] 'Renewing Scotland's Full Potential in the Digital World: Updating the Digital Strategy for Scotland - Discussion Document', Scottish Government, September 2020, p 8, available at https://www.gov.scot/publications/renewing-scotlands-full-potential-digital-world/

[49] UDHR Art. 12; see also, EU Charter of Fundamental Right Art. 7, European Convention on Human Rights Article 8

[50] Report of the Office of the United Nations High Commissioner for Human Rights to the Human Rights Council on 'The Right to Privacy in the Digital Age', 3 August 2018, A/HRC/39/29, p 1, available at https://undocs.org/A/HRC/39/29
[51]'Cambridge Analytica', Privacy International, available at https://privacyinternational.org/taxonomy/term/605; 'Facebook Data: How It Was Used by Cambridge Analytica' BBC News, 9 April 2018, available at https://www.bbc.com/news/av/technology-43674480 ; 'Cambridge Analytica Explained: Data and Elections', Privacy International, 13 April 2017, available at https://medium.com/privacy-international/cambridge-analytica-explained-data-and-elections-6d4e06549491 ; Green v SCL Group Ltd and others [2019] EWHC 954 (ch), [3], available at https://www.judiciary.uk/wp-content/uploads/2019/04/17.04.19-cambridge-judgment.pdf
[52] Dan Swinhoe, 'The 15 Biggest Data Breaches of the 21st century', CSO, 17 April 2020, available at https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
[53] 'Royal Free- Google DeepMind Trail Failed to Comply with Data Protection Law', ICO, 3 July 2017, available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/.

[54] Lorna McGregor, Vivian Ng and Ahmed Shaheed 'The Universal Declaration of Human Rights at 70: Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence, Human Rights Big Data and Technology Project, 20 December 2018, p 14, available at https://www.hrbdt.ac.uk/the-universal-declaration-of-human-rights-at-70-putting-human-rights-at-the-heart-of-the-design-development-and-deployment-of-artificial-intelligence/

[55] 'Background Paper on Consent Online', Human Rights, Big Data and Technology Project, August 2019, available at https://www.hrbdt.ac.uk/download/background-paper-on-consent/

[56] Patricia Norberg , Daniel Horne , David Horne :'The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors', The Journal of Consumer Affairs, 6 March 2007, available at https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-6606.2006.00070.x ; Ari Ezra Waldman, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'", New York Law School, 2020, available at https://digitalcommons.nyls.edu/fac_articles_chapters/1332

[57] Lorna McGregor, Vivian Ng and Ahmed Shaheed 'The Universal Declaration of Human Rights at 70: Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence, Human Rights Big Data and Technology Project, 20 December 2018, p 14, available at https://www.hrbdt.ac.uk/the-universal-declaration-of-human-rights-at-70-putting-human-rights-at-the-heart-of-the-design-development-and-deployment-of-artificial-intelligence/ ; 'Public Scrutiny of Automated Decisions: Early Lessons and Emerging Methods', An Upturn and Omidyar Network Report, 27 February 2018, available at https://omidyar.com/public-scrutiny-of-automated-decisions-early-lessons-and-emerging-methods/

[58]'The Humanitarian Metadata Problem: "Doing No Harm "in the Digital Era', Privacy International, October 2018, available at https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf

[59] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/73/348, 29 August 2018, p 13, available at https://www.undocs.org/A/73/348; Report of the Office of the United Nations High Commissioner for Human Rights to the Human Rights Council on 'The right to privacy in the digital age', 3 August 2018, A/HRC/39/29, p 1, available at https://undocs.org/A/HRC/39/29

[60] 'Applying the UN Guiding Principles on Business and Human Rights to Digital Technologies', OHCHR, November 2019, p 2, available at https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Project_revised_scoping_final.pdf

[61] ICCPR Article 26, also in UDHR Art 7, ICESCR Art 2

[62] Report of the UN High Commissioner for Human Rights on 'Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests', 24 June 2020, A/HRC/44/24, available at https://undocs.org/en/a/hrc/44/24

[63] Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, on 'Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis", 18 June 2020, A/HRC/44/57 Para 6, Available at https://undocs.org/en/A/HRC/44/57

[64] Joy Buolamwini, and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', Conference on Fairness, Accountability, and Transparency, 2018, available at http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf ; Steve Lohr, 'Facial Recognition Is Accurate, if You're a White Guy', New York Times, 9 February 2018, available at https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

[65] 'Home Office Says It Will Abandon Its Racist Visa Algorithm - After We Sued Them.', Foxglove, 4 August 2020, available at https://www.foxglove.org.uk/news/home-office-says-it-will-abandon-its-racist-visa-algorithm-nbsp-after-we-sued-them

[66] 'Home Office Says It Will Abandon Its Racist Visa Algorithm - After We Sued Them.', Foxglove, 4 August 2020, available at https://www.foxglove.org.uk/news/home-office-says-it-will-abandon-its-racist-visa-algorithm-nbsp-after-we-sued-them

[67] Report of the UN High Commissioner for Human Rights on 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests', 24 June 2020, A/HRC/44/24, available at https://undocs.org/en/a/hrc/44/24 ; Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, on 'Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis", 18 June 2020, A/HRC/44/57 Para 4, available at https://undocs.org/en/A/HRC/44/57

[68] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348, 29 August 2018, available at https://www.undocs.org/A/73/348 P 14 para 37 ; Ariana Tobin, "Why We Had to Buy Racist, Sexist, Xenophobic, Ableist and Otherwise Awful Facebook Ads," ProPublica, 27 November 2017, available at https://www.propublica.org/article/why-we-had-to-buy-racist-sexist-xenophobicableist-and-otherwise-awful-facebook-ads

[69] Paris Martineau, "YouTube's Search Suggests Racist Autocompletes", The Outline, 13 May 2018, available at https://theoutline.com/post/4536/youtube-s-search-autofill-suggests-racistresults?zd=1&zi=3ygzt6hw. Nicolar Kayser-Bril, 'Ten Years On, Search Auto-Complete Still Suggests Slander and Disinformation', AlgorithmWatch, 3 June 2020, available at https://algorithmwatch.org/en/story/auto-completion-disinformation/

[70] ICCPR Art 19 (1) (2)
[71] Human Rights Council Resolution, A/HRC/RES/25/2, 9 April 2014, available at https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session25/Pages/ResDecStat.aspx

[72] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to the General Assembly on 'Hate Speech', A/74/786, 9 October 2019, p 6, available at https://undocs.org/A/74/486

[73] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348, 29 August 2018, para 29, available at https://www.undocs.org/A/73/348

[74] Lorna McGregor, Vivian Ng and Ahmed Shaheed 'The Universal Declaration of Human Rights at 70: Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence, Human Rights Big Data and Technology Project, 20 December 2018, p 17, available at https://www.hrbdt.ac.uk/the-universal-declaration-of-human-rights-at-70-putting-human-rights-at-the-heart-of-the-design-development-and-deployment-of-artificial-intelligence/ 15; Asaf Lubin, '"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance', Chicago Journal of International Law, 2018, 18, 502, available at https://chicagounbound.uchicago.edu/cjil/vol18/iss2/3/ ; Ashley Deeks, 'An International Legal Framework for Surveillance', Virginia Journal of International Law, 2015, p 291, available at https://www.ilsa.org/Jessup/Jessup16/Batch%202/DeeksLegalFramework.pdf

[75] Daragh Murray and Pete Fussey, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data', Israel Law Review, 10 May 2019, available at https://www.hrbdt.ac.uk/download/bulk-surveillance-in-the-digital-age-rethinking-the-human-rights-law-approach-to-bulk-monitoring-of-communications-data/
[76] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, on 'Surveillance and Human Rights', A/HRC/41/35, 28 May 2019, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

[77]Fieke Jansen, 'Data Driven Policing in the Context of Europe', Cardiff University, 7 may 2018, p 2, available at https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf
[78]'Meeting Report: PHRP Expert Meeting on Predictive Policing', European Commission, 20 September 2019, available at https://ec.europa.eu/knowledge4policy/publication/meeting-report-phrp-expert-meeting-predictive-policing_en
[79] Submission to the UK Home Affairs Committee inquiry into 'Policing for the Future: Changing Demands and New Challenges', Human Rights Big Data and Technology Project, February 2017, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/policing-for-the-future-changing-demands-and-new-challenges/written/47227.html ; Ajay Sandhu, "Data Driven Policing: Highlighting Some Risks Associated with Predicting Crime", Human Rights Centre Blog, Essex University, 8 March 2017, available at https://hrcessex.wordpress.com/2017/03/08/data-driven-policing-highlighting-some-risks-associated-with-predicting-crime/
[80]'Problems with Crime Data', UK CrimeStats, available at https://www.ukcrimestats.com/AboutData/
[81] 'PHRP Expert Meeting on Predictive Policing', Amnesty International, 21 May 2019, available at https://ec.europa.eu/jrc/communities/sites/jrccties/files/expert-meeting-predictive-policing_may2019_report.pdf
[82] Lorna McGregor, Vivian Ng and Ahmed Shaheed 'The Universal Declaration of Human Rights at 70: Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence, Human Rights Big Data and Technology Project, 20 December 2018, p 25, available at https://www.hrbdt.ac.uk/the-universal-declaration-of-human-rights-at-70-putting-human-rights-at-the-heart-of-the-design-development-and-deployment-of-artificial-intelligence/; HRBDT, Written evidence to the UK Home Affairs Committee Inquiry on Policing for the Future, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/policing- for-the-future-changing-demands-and-new-challenges/written/47227.html ; 'Facial Recognition Technology and Predictive Policing Algorithms Out-Pacing the Law', Equality and Human Rights Commission, 12 March 2020, available at https://www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law
[83] Report of the UN High Commissioner for Human Rights on 'Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests', 24 June 2020, A/HRC/44/24, available at https://undocs.org/en/a/hrc/44/24
[84] Ibid para 31
[85] Ibid. para 32
[86] Sandhu, A., and Fussey, P. (2020) 'The Uberization of Policing', Policing and Society, Online First, p5-6, available at doi.org/10.1080/10439463.2020.1803315
[87] 'UN Expert Joins Call for Immediate Moratorium on Sale, Transfer and Use of Surveillance Tech', UN News, 15 July 2020, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26098&LangID=E; https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736
[88] Ibid.
[89] 'Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance', Amnesty International, 11 June 2020, available at https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/#:~:text=In%20the%20context%20of%20racially,and%20the%20right%20to%20privacy. ; Karen Weise and Natasha Singer, 'Amazon Pauses Police Use of Its Facial Recognition Software', The New York Times, 10 June 2020, available at https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html
[90] Report of the Special rapporteur on the right to education on the 'Impact of the Coronavirus Disease Crisis on the Right to Education- Concerns, Challenges and Opportunities', A/HRC/44/39, 30 June 2020, available at https://undocs.org/A/HRC/44/39
[91] Report of the Special rapporteur on the right to education to the Human rights Council, A/HRC/32/37, 6 April 2016, available at https://undocs.org/A/HRC/32/37 para 36, para 69
[92] Ibid. para 92 and 93
[93] Hye Jung Han, "As Schools Close over Coronavirus, Protect Kids' Privacy in Online Learning", Human

Rights Watch, 27 March 2020, available at https://www.hrw.org/news/2020/03/27/schools-close-over-coronavirus-protect-kids-privacy-online-learning ; Report of the Special Rapporteur on the right to education on the 'Impact of the Coronavirus Disease Crisis on the Right to Education- Concerns, Challenges and Opportunities', A/HRC/44/39, 30 June 2020, para 49, available at https://undocs.org/A/HRC/44/39

[94] The Abidjan Principles, adopted 13 February 2019, Abidjan, Côte D'Ivoire, available at https://www.abidjanprinciples.org/#:~:text=The%20Abidjan%20Principles&text=On%2012%2D13%20February%202019.participatory%20consultation%20and%20drafting%20process

[95] Ibid.

[96] Ibid.

[97] Report of the Special Rapporteur on extreme poverty and human rights, Philip Alston, on 'Extreme Poverty and Human Rights', A/74/493, 11 October 2019, available at https://undocs.org/pdf?symbol=en/A/74/493

[98] Report of the Special Rapporteur on extreme poverty and human rights to the General Assembly, A/74/49, 11 October 2019, para 5, available at https://undocs.org/pdf?symbol=en/A/74/493

[99] 'Computer Says No! Access to Justice and Digitalisation in Universal Credit', Child Poverty Action Group, 1 May 2019, available at https://cpag.org.uk/policy-and-campaigns/computer-says-no-access-justice-and-digitalisation-universal-credit

[100] 'SyRI case, Rechtsbank Den Haag, 5 February 2020, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878 ; 'The SyRI Case: A Landmark Ruling for Benefits Claimants around the World', Privacy International, 24 February 2020, available at https://privacyinternational.org/news-analysis/3363/syri-case-landmark-ruling-benefits-claimants-around-world

[101] Nani Jansen Reventlow, 'Tackling the Human Rights Impacts of the 'Digital Welfare State', 10 February 2020, available at https://digitalfreedomfund.org/tackling-the-human-rights-impacts-of-the-digital-welfare-state/ ; Tom Wills, 'Sweden: Rogue Algorithm Stops Welfare Payments for up to 70,000 Unemployed', 25 February 2020, Algorithm Watch, available at https://algorithmwatch.org/en/rogue-algorithm-in-sweden-stops-welfare-payments/

[102] Luke Henriques-Gomes, 'The Automated System Leaving Welfare Recipients Cut off with Nowhere to Turn' The Guardian, 16 October 2019), available at https://www.theguardian.com/technology/2019/oct/16/automated-messages-welfare-australia-system

[103] Robert Booth, 'Benefits System Automation Could Plunge Claimants Deeper into Poverty', The Guardian, 14 October 2019, available at https://www.theguardian.com/technology/2019/oct/14/fears-rise-in-benefits-system-automation-could-plunge-claimants-deeper-into-poverty

[104] 'UK: Automated Benefits System Failing People in Need' Human Rights Watch, 29 September 2020, available at https://www.hrw.org/news/2020/09/29/uk-automated-benefits-system-failing-people-need ; Full report available at https://www.hrw.org/report/2020/09/29/automated-hardship/how-tech-driven-overhaul-uks-social-security-system-worsens

[105] 'Automating Hardship: How the Tech-Driven Overhaul of the UK's Social Security System Worsen Poverty', Human Rights Watch, 29 September 2020, available at https://www.hrw.org/report/2020/09/29/automated-hardship/how-tech-driven-overhaul-uks-social-security-system-worsens

[106] ICCPR Article 2(3) and UNGPs pillar 3

[107] Dan Sabbagh, 'South Wales Police Lose Landmark Facial Recognition Case', 11 August 2020, available at https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recognition-case

[108] Report of the Special Rapporteur on extreme poverty and human rights, Philip Alston, on 'Extreme Poverty and Human Rights', A/74/493, 11 October 2019, available at https://undocs.org/pdf?symbol=en/A/74/493 ,

[109] UNGP Pillar 2, available at https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

[110] These principles build on our report, Lorna McGregor, Vivian Ng and Ahmed Shaheed, 'The Universal Declaration of Human Rights at 70: Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence, Human Rights Big Data and Technology Project, 20 December 2018, p 17, available at https://www.hrbdt.ac.uk/the-universal-declaration-of-human-rights-at-70-putting-human-rights-at-the-heart-of-the-design-development-and-deployment-of-artificial-intelligence/ and are further elaborated in our forthcoming report, Lorna McGregor, Elena Abrusci, et al, 'Placing Human Rights Principles at the Heart of National AI Strategies' *forthcoming* 2021.See also, Charles Bradley, Richard Wingfield, Megan Metzger, 'National Artificial Intelligence

Strategies and Human Rights: A Review' *Global Partners Digital and Stanford Global Digital Policy Incubator* April 2020: available at: https://cyber.fsi.stanford.edu/gdpi/content/national-artificial-intelligence-strategies-and-human-rights-review

[111] 'A Human Rights Based Approach: PANEL Principles', Scottish Human Rights Commission, available at https://www.scottishhumanrights.com/media/1409/shrc_hrba_leaflet.pdf

[112] 'Our Response to the European Commission's Consultation on AI', Algorithm Watch, 12 June 2020, available at https://algorithmwatch.org/en/response-european-commission-ai-consultation/

[113] Lorna McGregor, Daragh Murray and Vivian Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability', International and comparative Law Quarterly, 17 April 2019, available at https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/international-human-rights-law-as-a-framework-for-algorithmic-accountability/1D6D0A456B36BA7512A6AFF17F16E9B6

[114] UN Guiding Principles on Business and Human Rights, Pillar I and II, available at https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

[115] 'Guidance on human rights impact assessments of digital activities', The Danish Institute for Human Rights, p 38, available at https://www.humanrights.dk/sites/humanrights.dk/files/media/document/A%20HRIA%20of%20Digital%20Activities%20-%20Introduction_n.pdf; Lorna McGregor and Sabrina Rau, "Identification of Synergies and Divergences between HRIA and DPIA: Assessing Entry Points for Human Rights Integration", Human Rights Big Data and Technology Project (forthcoming)

[116] UNGP Pillar 3, available at https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

[117] 'Expert Meeting on the Technology Sector and Access to Remedy through Non-State-Based Grievance Mechanisms', Human Rights, Big Data and Technology Project and OHCHR, 11 June 2019, available at https://www.ohchr.org/Documents/Issues/Business/B-Tech/HRBDTOHCHRExpertMeetingTunis6September2019.pdf

[118] Anna Jobin, Marcello Lenca, and Effy Vayena, 'The Global Landscape of AI Ethics Guidelines' Nature Machine Intelligence, June 2019, available at https://www.researchgate.net/publication/334082218_Artificial_Intelligence_the_global_landscape_of_ethics_guidelines

[119] Ibid.

[120] Lorna McGregor, Elena Abrusci, et al, 'Placing Human Rights Principles at the Heart of National AI Strategies' *forthcoming* 2021.

[121] Ibid.

[122] Ibid.

[123] Ibid.

[124] Ibid.

[125] Ibid.

[126] Ibid.

[127] Ibid.

[128] Ibid.

[129] Ibid.

[130] Ibid.

[131] Ibid.

[132] Ibid.

[133] Ibid.

[134] Ibid.

[135] Ibid.

[136] Ibid.

[137] Ibid.

[138] Ibid.

[139] Ibid.

[140] Ibid.

[141] Ibid.

[142] Ibid.

[143] Lorna McGregor and Ahmed Shaheed, 'The COVID-19 Pandemic: Five Urgent Principles for Leaving No One Behind through Technology', 19 May 2020, available at https://www.universal-rights.org/blog/the-covid-19-pandemic-five-urgent-principles-for-leaving-no-one-behind-through-technology/

[144] 'Guidance on human rights impact assessments of digital activities', The Danish Institute for Human Rights, p 38, available at https://www.humanrights.dk/sites/humanrights.dk/files/media/document/A%20HRIA%20of%20Digital%20Activities%20-%20Introduction_n.pdf;