United Nations A/74/493

General Assembly

Distr.: General
11 October 2019

Original: English

Seventy-fourth session
Agenda item 70 (b)
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Extreme poverty and human rights*

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report of the Special Rapporteur on extreme poverty and human rights, Philip Alston, submitted in accordance with Human Rights Council resolution 35/19.

* The present report was submitted after the deadline in order to reflect the most recent developments.

19-17564 (E) 291019

Please recycle

Report of the Special Rapporteur on extreme poverty and human rights

Summary

The digital welfare state is either already a reality or emerging in many countries across the globe. In these states, systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish. In the present report, the irresistible attractions for Governments to move in this direction are acknowledged, but the grave risk of stumbling, zombie-like, into a digital welfare dystopia is highlighted. It is argued that big technology companies (frequently referred to as "big tech") operate in an almost human rights-free zone, and that this is especially problematic when the private sector is taking a leading role in designing, constructing and even operating significant parts of the digital welfare state. It is recommended in the report that, instead of obsessing about fraud, cost savings, sanctions, and market-driven definitions of efficiency, the starting point should be on how welfare budgets could be transformed through technology to ensure a higher standard of living for the vulnerable and disadvantaged.

Contents

I. Introduction[1]

1. The era of digital governance is upon us. In high- and middle-income countries, electronic voting, technology-driven surveillance and control, including through facial recognition programmes, algorithm-based predictive policing, the digitization of justice and immigration systems, online submission of tax returns and payments and many other forms of electronic interactions between citizens and different levels of government are becoming the norm. In lower-income countries, national systems of biometric identification are laying the foundations for comparable developments, especially in systems to provide social protection, or "welfare", to use a shorthand term.[2]

2. Invariably, improved welfare provision, along with enhanced security, is one of the principal goals invoked to justify the deep societal transformations and vast expenditure that are involved in moving the entire population of a country not just on to a national unique biometric identity card system but also into linked centralized systems providing a wide array of government services and goods ranging from food and education to health care and special services for the ageing and for persons with disabilities.

3. The result is the emergence of the "digital welfare state" in many countries across the globe.[3] In these countries, systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish. The process is commonly referred to as "digital transformation", but this somewhat neutral term should not be permitted to conceal the revolutionary, politically driven character of many such innovations. Commentators have predicted "a future in which government agencies could effectively make law by robot",[4] and it is clear that new forms of governance are emerging which rely significantly on the processing of vast quantities of digital data from all available sources, use predictive analytics to foresee risk, automate decision-making and remove discretion from human decision makers. In such a world, citizens become ever more visible to their Governments, but not the other way around.[5]

4. Welfare is an attractive entry point not just because it takes up a major share of the national budget or affects such a large proportion of the population but because digitization can be presented as an essentially benign initiative. Thus, for example, the Government Transformation Strategy of the United Kingdom of Great Britain and Northern Ireland proclaims that it is intended to transform the relationship between citizens and the State, putting more power in the hands of citizens and being more responsive to their needs. The core values of the Unique Identification Authority of India include facilitating good governance, integrity, inclusive nation-building, a collaborative approach, excellence in services and transparency and openness.

5. In other words, the embrace of the digital welfare state is presented as an altruistic and noble enterprise designed to ensure that citizens benefit from new

[1] The present report has been prepared in close collaboration with Christiaan van Veen, Director of the Digital Welfare States and Human Rights Project at New York University School of Law.

[2] While "welfare" is often used as a pejorative term, it is used in a positive sense in the present report and is synonymous with the goal of social protection as reflected in the Social Protection Floor Initiative and comparable approaches. See David Garland, *The Welfare State: A Very Short Introduction* (Oxford, Oxford University Press, 2016).

[3] Philip Alston and Christiaan van Veen, "How Britain's welfare state has been taken over by shadowy tech consultants", *Guardian*, 27 June 2019.

[4] Cary Coglianese and David Lehr, "Regulating by robot: administrative decision making in the machine-learning era", *Georgetown Law Journal*, vol. 105, No. 5 (July 2017), p. 1147.

[5] See Foucault's description of panoptic systems, in which those put under surveillance are "seen, without ever seeing" (Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York, Pantheon Books, 1977), p. 202).

technologies, experience more efficient governance and enjoy higher levels of well-being. Often, however, the digitization of welfare systems has been 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 behavioural 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.

6. These other outcomes are promoted in the name of efficiency, targeting, incentivizing work, rooting out fraud, strengthening responsibility, encouraging individual autonomy and responding to the imperatives of fiscal consolidation. Through the invocation of what are often ideologically charged terms, neoliberal economic policies are seamlessly blended into what are presented as cutting-edge welfare reforms, which in turn are often facilitated, justified and shielded by new digital technologies. Although the latter are presented as being "scientific" and neutral, they can reflect values and assumptions that are far removed from, and may be antithetical to, the principles of human rights. In addition, because of the relative deprivation and powerlessness of many welfare recipients, conditions, demands and forms of intrusiveness are imposed that would never be accepted if they were piloted in programmes applicable to better-off members of the community instead.

7. Despite the enormous stakes involved, not just for millions of individuals but for societies as a whole, these issues have, with a few notable exceptions,[6] garnered remarkably little attention. The mainstream technology community has been guided by official preoccupations with efficiency, budget savings and fraud detection. The welfare community has tended to see the technological dimensions as separate from policy developments, rather than as being integrally linked. Lastly, those in the human rights community concerned with technology have understandably been focused instead on concerns such as the emergence of the surveillance state, the potentially fatal undermining of privacy, the highly discriminatory impact of many algorithms and the consequences of the emerging regime of surveillance capitalism.

8. However, the threat of a digital dystopia is especially significant in relation to the emerging digital welfare state. The present report is aimed at redressing the neglect of these issues to date by providing a systematic account of the ways in which digital technologies are used in the welfare state and of their implications for human rights. It concludes with a call for the regulation of digital technologies, including artificial intelligence, to ensure compliance with human rights and for a rethinking of the positive ways in which the digital welfare state could be a force for the achievement of vastly improved systems of social protection.

9. The report builds in part on reports by the Special Rapporteur on visits to the United States of America in 2017 (A/HRC/38/33/Add.1) and the United Kingdom in 2018 (A/HRC/41/39/Add.1), in which attention was drawn to the increasing use of digital technologies in social protection systems. In preparing the present report, the Special Rapporteur consulted representatives of various digital rights groups, leading scholars and other stakeholders, first in a meeting hosted by the Digital Freedom Fund in Berlin in February 2019, and then at a meeting sponsored by the Center for Information Technology Policy at Princeton University, United States, in April 2019. In addition, a formal call for contributions resulted in some 60 submissions from 22 Governments, as well as international and national civil society organizations,

[6] For pioneering work on the impact of digital technologies on the welfare state in the United States, especially on the poorest individuals in the system, see Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York, St Martin's Press, 2018). See also Cathy O'Neil, *Weapons of Math Destruction* (New York, Crown, 2016); and Khiara Bridges, *The Poverty of Privacy Rights* (Stanford, California, Stanford University Press, 2017).

national human rights institutions, academics and individuals in 34 countries.[7] While it is impossible to do justice to these rich and detailed submissions in such a necessarily brief report, the Special Rapporteur has made them available electronically[8] and will continue analysing them in the context of his team's ongoing work on the digital welfare state.[9]

II. Uses of digital technologies in the welfare state

10. From the many submissions received, and on the basis of various case studies addressed in the literature, it is possible to distinguish various ways, and different stages in the welfare context, in which digital innovation has been used most prominently.

A. Identity verification

11. Establishing every person's legal identity, including through birth registration, by 2030 is target 16.9 of the Sustainable Development Goals. A verifiable identity is essential for applying for benefits, establishing entitlements, receiving benefits and appealing against denial of benefits. For the Government or other provider, a verifiable identity avoids duplication and fraud, facilitates accurate targeting and enhances efficiency. Traditionally, paper and/or plastic documents have been used in forms such as birth certificates, identity cards and passports. These systems function reasonably well in most of the global North, although 21 million adults in the United States do not have government-issued photo identification.[10] In the global South, 502 million people in sub-Saharan Africa and 357 million people in South Asia lack official identification.[11] In Liberia, for example, birth registration stands at only 5 per cent and national identity cards were not introduced until 2015.[12]

12. In response, the World Bank, regional development organizations and bilateral donors have launched new programmes to promote access to identity documents. In particular, the World Bank's Identification for Development (ID4D) campaign has focused heavily on promoting digital technologies. The role of digital technology in identity documents is set out in the "Principles on identification for sustainable development: toward the digital age", which were facilitated by the World Bank and the Center for Global Development and have been widely endorsed, including by MasterCard.

13. It is acknowledged in the Principles that both advantages and disadvantages are involved. On the positive side, it is claimed that digital technology can create huge savings for citizens, Governments and businesses by reducing transaction costs, increasing efficiency and driving innovation in service delivery, particularly to the poorest and most disadvantaged groups in society. It is also noted that digital identity systems can also improve governance, boost financial inclusion, reduce gender

[7] Argentina, Australia, Austria, Azerbaijan, Brazil, Chile, Croatia, Egypt, El Salvador, Estonia, Germany, Greece, Guatemala, India, Italy, Ireland, Kazakhstan, Lebanon, Mexico, Nicaragua, Nigeria, Netherlands, New Zealand, Oman, Pakistan, Philippines, Poland, Qatar, Russian Federation, Senegal, South Africa, Switzerland, United Kingdom and United States.

[8] www.ohchr.org/EN/Issues/Poverty/Pages/SubmissionsGADigitalTechnology.aspx.

[9] https://chrgj.org/people/christiaan-van-veen/.

[10] Wendy R. Weiser and Lawrence Norden, *Voting Law Changes in 2012* (New York, Brennan Center for Justice at New York University School of Law, 2011), p. 2.

[11] United States Agency for International Development, *Identity in a Digital Age: Infrastructure for Inclusive Development* (2017), p. 8.

[12] Bronwen Manby, *Citizenship in Africa: The Law of Belonging* (Oxford, Hart Publishing, 2018), p. 3.

inequalities by empowering women and girls, and increase access to health services and social safety nets for the poor (p. 5).

14. However, in addition to this impressive and by now familiar sales pitch, possible risks are recognized in the Principles, and similar documents.[13] Those risks range from political backlash to concerns over privacy, security and cybersecurity. Solutions for dealing with those risks are often technological or take the form of soft law norms. The United States Agency for International Development has called for open source solutions and the development of good practices for data privacy to resolve the relevant problems.[14] While the "Principles on identification for sustainable development" contain references to human rights principles such as article 7 of the Convention on the Rights of the Child, emphasis is placed primarily on the need to create an interoperable platform using open standards, and protecting privacy through system design.

15. The world's largest biometric identification system is Aadhaar in India. Residents are issued a 12-digit unique identifying number and the system contains both demographic and biometric information, including an iris scan, a photograph and fingerprints. It is used to verify the identity of recipients of benefits and subsidies and is now mandatory to access those social rights. It was first introduced in 2009 and now covers more than 1.2 billion people.[15] It has been enthusiastically endorsed by the international development community.[16] The World Bank has praised it for overcoming complex information problems, thereby helping willing Governments to promote the inclusion of disadvantaged groups,[17] and has encouraged other Governments to learn from the experience.[18] Over 20 countries are reported to have expressed an interest in emulating Aadhaar.[19]

16. It nevertheless remains controversial domestically. Critics of Aadhaar have reportedly been harassed and surveilled,[20] and the scheme has been criticized for collecting biometric information unnecessarily, severe shortcomings in legislative oversight, function creep, facilitating surveillance and other intrusions into privacy, exacerbating cybersecurity issues and creating barriers to accessing a range of social rights.[21]

17. In 2018, the Supreme Court of India, in a 1,448-page landmark ruling, upheld the constitutionality of Aadhar, albeit with some caveats. The court appeared to view the use of biometric identification technology in the context of providing welfare benefits as being legitimate, proportional and even inevitable. In a welfare state, Aadhaar's aim of ensuring that benefits reach the intended beneficiary was "naturally a legitimate State aim".[22] In balancing the rights to social security and privacy, the

[13] *Identity in a Digital Age*; and McKinsey Global Institute, "Digital identification: a key to inclusive growth" (January 2019).

[14] *Identity in a Digital Age*.

[15] Rahul Tripathi, "National population register to include Aadhaar details", *Economic Times*, 5 August 2019.

[16] Jeanette Rodrigues, "India ID program wins World Bank praise despite 'Big Brother' fears", Bloomberg, 16 March 2017.

[17] World Bank, *World Development Report 2016: Digital Dividends* (Washington, D.C., 2016), p. 2.

[18] Amrit Raj and Upasana Jain, "Aadhaar goes global, finds takers in Russia and Africa", Live Mint, 9 July 2016.

[19] Jayadevan PK, "India's latest export: 20 countries interested in Aadhaar, India Stack", Factory Daily, 10 January 2018.

[20] Rahul Bhatia, "Critics of India's ID card project say they have been harassed, put under surveillance", Reuters, 13 February 2018.

[21] Submission to the Special Rapporteur by the Centre for Communication Governance at the National Law University, Delhi.

[22] Supreme Court of India, *Justice K.S. Puttaswamy and Another v. Union of India and Others*, Writ Petition (Civil) No. 494 of 2012, p. 341.

Court held that registering biometric data represented a minimal inroad into privacy rights[23] and went so far as to characterize Aadhaar as a vital tool for ensuring good governance in a social welfare state.[24] However, the Supreme Court's ruling has apparently not put an end to the controversy surrounding the scheme.[25]

18. In 2019, Kenya required all of its citizens, including those living abroad, and all foreign nationals and refugees in the country above the age of 6 to obtain a national identification card in order to access government services, including welfare benefits. This involved providing biometric data including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and DNA in digital form. In response to a case claiming that the National Integrated Identity Management System (NIIMS), also known as Huduma Namba (Swahili for "service number"), violated the rights to privacy, equality, non-discrimination and public participation, the High Court issued an interim order allowing the registration process to continue, but on a voluntary basis and on the basis that the disbursement of government services and benefits could not be made conditional on participation. Subsequently, registration has proceeded apace: nearly two thirds of the population has been registered,[26] and the Government is reportedly threatening to withdraw unregistered individuals' access to benefits and the right to vote.[27]

19. In South Africa, the South African Social Security Agency distributes non-contributory and means-tested social grants, including grants for child support, for pensioners and for persons with disabilities, to about one third of the population.[28] In 2012, the Agency contracted the company Cash Paymaster Services, a subsidiary of Net1, to deliver the grants.[29] Cash Paymaster Services registered beneficiaries by collecting their biometric information (fingerprints and, originally, voice recordings) and beneficiaries were issued MasterCard debit cards with biometric functionality and a linked bank account by Net1 and Grindrod Bank in association with the Agency.[30] After much controversy surrounding the tender to Cash Paymaster Services, the fees charged by the company, deductions made to social grants on these accounts and privacy concerns surrounding the processing of cardholder data, the Agency changed providers in 2018 by entering into a partnership with the South African Post Office. The Agency and the Post Office will provide new biometric cards. The change from Cash Paymaster Services to the Post Office has been complex and has led to questions about effective access to social grants by beneficiaries in South Africa.[31]

[23] Ibid., p. 377.
[24] Ibid., p. 553.
[25] Vindu Goel, "India's top court limits sweep of biometric ID programme", *New York Times*, 26 September 2018.
[26] Submission to the Special Rapporteur by Amnesty International.
[27] Moses Nyamori, "No healthcare, voting without Huduma Namba, bill proposes", Standard Digital, 18 July 2019.
[28] Mary Jan Mphahlele, "#BUDGET2019: social grants to increase", *Diamond Fields Advertiser*, 20 February 2019.
[29] Submission to the Special Rapporteur by Black Sash.
[30] Mastercard, "More than 2.5 million Mastercard debit cards issued to social welfare beneficiaries in South Africa", press release, 30 July 2012.
[31] Ray Mahlaka, "Post office set to take over cash payments from CPS", *The Citizen*, 4 June 2018.

20. Many other examples could be given of countries using or exploring digital identity systems, including Argentina,[32] Bangladesh,[33] Chile,[34] Ireland,[35] Jamaica,[36] Malaysia,[37] the Philippines[38] and the United States.[39]

B. Eligibility assessment

21. Automated programmes are increasingly used to assess eligibility in many countries. An especially instructive case was the automation of eligibility decisions in Ontario, Canada, in 2014 through the Social Assistance Management System, which was based on Cúram, a customizable, off-the-shelf IBM software package also used in welfare programmes in Australia, Germany, New Zealand and the United States.[40]

22. In 2015, the Auditor-General of Ontario reported on 1,132 cases of errors with eligibility determinations and payment amounts under the Social Assistance Management System, involving about 140 million Canadian dollars. The total expenditure on the System by late 2015 was 290 million Canadian dollars.[41] The new system reportedly led caseworkers to resort to subterfuge to ensure that beneficiaries were fairly treated; it also made decisions very difficult to understand and created significant additional work for staff.[42]

C. Welfare benefit calculation and payments

23. The calculation and payment of benefits is increasingly done using digital technologies without the involvement of caseworkers and other human decision makers. While such systems offer many potential advantages, the Special Rapporteur also received information about prominent examples of system errors or failures that had generated major problems for large numbers of beneficiaries. These included the automated debt-raising and recovery system ("robo-debt") in Australia,[43] the Real Time Information system in the United Kingdom[44] and the Social Assistance Management System in Canada.

24. Electronic payment cards or debit cards are increasingly being issued to welfare recipients. Information provided to the Special Rapporteur in relation to such programmes in Australia, New Zealand and South Africa reveal very similar

[32] Submission to the Special Rapporteur by the Government of Argentina.
[33] Privacy International, "Bangladesh: biometrics needed to access welfare payment", 2 May 2017.
[34] In Chile, facial recognition technology is used to deliver school meals (submission to the Special Rapporteur by Privacy International).
[35] Submission to the Special Rapporteur by the Government of Ireland.
[36] See the National Identification System webpage (https://opm.gov.jm/portfolios/national-identification-system).
[37] Alita Sharon, "Malaysia's digital ID project to be finalized by 2019", Open Gov, 10 June 2019.
[38] See the Philippine Identification System webpage (https://psa.gov.ph/philsys).
[39] For example, the use of digital technologies in the CalWORKs programme in California (submission to the Special Rapporteur by Human Rights Watch).
[40] Submission to the Special Rapporteur by Human Rights Watch.
[41] Canada, Office of the Auditor General of Ontario, *Annual Report 2015* (Toronto, Ontario, Queen's Printer for Ontario, 2015), p. 475.
[42] Jennifer Raso, "Displacement as regulation: new regulatory technologies and front-line decision-making in Ontario works", *Canadian Journal of Law and Society*, vol. 32, No. 1 (2017), pp. 75–95.
[43] Terry Carney, "The new digital future for welfare: debts without legal proofs or moral authority?", UNSW Law Journal Forum (March 2018); Richard Glenn, *Centrelink's Automated Debt Raising and Recovery System* (2017), pp. 7–8; and submission to the Special Rapporteur by the Castan Centre for Human Rights Law at Monash University.
[44] Philip Alston, Special Rapporteur on extreme poverty and human rights, statement on visit to the United Kingdom of Great Britain and Northern Ireland, 16 November 2018.

problems. First, beneficiaries often face difficulties accessing and fully utilizing their right to social security.[45] Second, when such cards are clearly recognizable as welfare-related, users have expressed feelings of disempowerment, embarrassment and shame,[46] a problem exacerbated when the users come from communities long accustomed to exclusion.[47] Third, electronic cards enable monitoring and surveillance of behavioural data by welfare authorities and private actors, thus raising important human rights concerns.[48]

25. Moreover, the outsourcing of the issuance and administration of electronic cards to private companies has led to problems such as users being encouraged to pay for commercial financial products and the imposition of user fees.[49] More generally, the ethos surrounding such cards has often reflected stereotypes such as the financial untrustworthiness and irrationality of those living in poverty.

D. Fraud prevention and detection

26. Fraud and error in welfare systems can potentially involve very large sums of money and have long been a major concern for Governments. It is thus unsurprising that many of the digital welfare systems that have been introduced have been designed with a particular emphasis on the capacity to match data from different sources in order to expose deception and irregularities on the part of welfare applicants. Nevertheless, evidence from country missions undertaken by the Special Rapporteur,[50] along with other cases examined,[51] suggests that the magnitude of these problems is frequently overstated and that there is sometimes a wholly disproportionate focus on this particular dimension of the complex welfare equation. Images of supposedly wholly undeserving individuals receiving large government welfare payments, such as Ronald Reagan's "welfare queen" trope, have long been used by conservative politicians to discredit the very concept of social protection. The risk is that the digital welfare state provides endless possibilities for taking surveillance and intrusion to new and deeply problematic heights.

E. Risk scoring and need classification

27. Risk calculation is inevitably at the heart of the design of welfare systems, and digital technologies can achieve very high levels of sophistication in this regard. In addition to fraud detection and prevention, child protection has been a major focus in this area, as illustrated by examples from countries such as Denmark,[52] New Zealand,[53]

[45] Submission to the Special Rapporteur by Shelley Bielefeld (Griffith University).
[46] Submission to the Special Rapporteur by Nijole Naujokas.
[47] Melissa Davey, "'Ration days again': cashless welfare card ignites shame", *Guardian*, 8 January 2017.
[48] Submission to the Special Rapporteur by Louise Humpage (University of Auckland).
[49] Andries du Toit, "The real risks behind South Africa's social grant payment crisis", The Conversation, 20 February 2017.
[50] See, for example, Alston, statement on visit to the United Kingdom.
[51] For example, the case on system risk indication from the Netherlands (see Philip Alston, Special Rapporteur on extreme poverty and human rights, brief as amicus curiae before the District Court of the Hague on the case of *NJCM c.s./De Staat der Nederlanden (SyRI)*, case No. C/09/550982/ HA ZA 18/388, September 2019).
[52] Jacob Mchangama and Hin-Yan Liu, "The welfare state is committing suicide by artificial intelligence", Foreign Policy, 25 December 2018.
[53] Philip Gillingham, "Predictive risk modelling to prevent child maltreatment: insights and implications from Aotearoa/New Zealand", *Journal of Public Child Welfare*, vol. 11, No. 2 (2017).

the United Kingdom[54] and the United States.[55] Governments have also applied these techniques to determine whether unemployment assistance will be provided and at what level. A prominent such scheme in Poland was held unconstitutional,[56] but an algorithm-based system in Austria continues to categorize unemployed jobseekers to determine the support they will receive from government job centres.[57]

28. Many other areas of the welfare state will also be affected by new technologies used to score risks and classify needs.[58] While such approaches offer many advantages, it is also important to take into account the problems that can arise. First, there are many issues raised by determining an individual's rights on the basis of predictions derived from the behaviour of a general population group.[59] Second, the functioning of the technologies and how they arrive at a certain score or classification are often secret, thus making it difficult to hold Governments and private actors to account for potential rights violations.[60] Third, risk-scoring and need categorization can reinforce or exacerbate existing inequalities and discrimination.[61]

F. Communication between welfare authorities and beneficiaries

29. Communication that previously took place in person, by phone or by letter is increasingly being replaced by online applications and interactions. In various submissions to the Special Rapporteur, problems were cited with the Universal Credit system in the United Kingdom, including difficulties linked to a lack of Internet access and/or digital skills[62] and the extent to which online portals can create confusion and obfuscate legal decisions, thereby undermining the right of claimants to understand and appeal decisions affecting their social rights.[63] Similar issues have also been raised in relation to other countries, including Australia[64] and Greece.[65]

30. Another problem is the likelihood, once the entire process of applying and maintaining benefits is moved online, of the situation inviting further digital

[54] Niamh McIntryre and David Pegg, "Councils use 377,000 people's data in efforts to predict child abuse", *Guardian*, 16 September 2018; and Alex Turner, "County becomes latest authority to trial predictive algorithms in children's social work", Community Care, 14 June 2019.

[55] Eubanks, *Automating Inequality*; Alexandra Chouldechova and others, "A case study of algorithm-assisted decision making in child maltreatment hotline screening decisions", *Proceedings of Machine Learning Research*, vol. 81 (2018), pp. 1–5; and Dan Hurley, "Can an algorithm tell when kids are in danger?", *New York Times*, 2 January 2018.

[56] Supreme Court of Poland, case No. K 53/16, 6 June 2018.

[57] Submission to the Special Rapporteur by EpicenterWorks.

[58] See, for example, Lina Dencik and others, *Data Scores as Governance: Investigating Uses of Citizen Scoring in Public Services* (Data Justice Lab, Cardiff University, and Open Society Foundations, 2018).

[59] Household-level and individual-level data rely on a fundamental personalization of risk, attaching risk factors to individual characteristics and behaviour that can lead to individualized responses to social ills being privileged over collective and structural responses, such as issues of inequality, poverty or racism (submission to the Special Rapporteur by the Data Justice Lab at Cardiff University); and submission to the Special Rapporteur by Paul Henman (University of Queensland).

[60] Submission to the Special Rapporteur by Jędrzej Niklas and Seeta Peña Gangadharan (London School of Economics and Political Science).

[61] "Human bias is built in to the predictive risk model." (Virginia Eubanks, "A child abuse prediction model fails poor families", *Wired*, 15 January 2018).

[62] Submissions to the Special Rapporteur by the Scottish Council for Voluntary Organisations and Citizens Advice Scotland.

[63] Submission to the Special Rapporteur by the Child Poverty Action Group.

[64] Australia, Senate Community Affairs References Committee, *Design, Scope, Cost-Benefit Analysis, Contracts Awarded and Implementation Associated with the Better Management of the Social Welfare System Initiative* (Canberra, 2017), p. 60.

[65] Submission to the Special Rapporteur by the Government of Greece.

innovation. In 2018, Sweden was forced to reverse a complex digital system used by the Employment Service to communicate with jobseekers because of problems that led to as many as 15 per cent of the system's decisions likely being incorrect.[66]

31. In Australia, the Targeted Compliance Framework requires jobseekers to use a digital dashboard to report mandatory activities and to check their compliance status. Failure to meet a "mutual obligation" can automatically, without the involvement of a human decision maker, lead to the suspension of payments or the imposition of financial penalties. Problems have been highlighted that result from a lack of Internet access and digital literacy and to the rigidity of an automated system which fails to take real-life situations into account.[67]

III. Making digital technologies work for social protection

32. Digital technologies, including artificial intelligence, have huge potential to promote the many benefits that are consistently cited by their proponents. They are already doing so for those who are economically secure and can afford to pay for the new services. They could also make an immense positive difference by improving the well-being of the less well-off members of society, but this will require deep changes in existing policies. The leading role in any such effort will have to be played by Governments through appropriate fiscal policies and incentives, regulatory initiatives and a genuine commitment to designing the digital welfare state not as a Trojan Horse for neoliberal hostility towards welfare and regulation but as a way to ensure a decent standard of living for everyone in society.

33. In the present report, problems that are specific to the ways in which the digital welfare state has been envisioned and implemented have been highlighted. However, many of the changes required to avoid a digital dystopia will need to range more broadly. In addressing the General Assembly on 24 September 2019, the Prime Minister of the United Kingdom warned of the dangers of the digital age, singling out: (a) the risk of round-the-clock surveillance; (b) the perils of algorithmic decision-making; (c) the difficulty of appealing against computer-generated determinations; and (d) the inability to plead extenuating circumstances when the decision maker is an algorithm. He concluded rather ominously by suggesting that digital authoritarianism was an emerging reality.[68]

34. His comments resonate strongly in the context of the digital welfare state, including in relation to the Universal Credit system of the United Kingdom. There is no magic recipe for avoiding the pitfalls of which he warned, but the steps set out in the following subsections could help to make the digital welfare state a force for enhancing rather than undermining human rights.

A. Taking human rights seriously and regulating accordingly

35. The Prime Minister of the United Kingdom concluded his statement to the General Assembly by warning that, unless new technology reflected the rights contained in the Universal Declaration of Human Rights, that Declaration would mean

[66] Tom Wills, "Sweden: rogue algorithm stops welfare payments for up to 70,000 unemployed", Algorithm Watch, 19 February 2019.

[67] Submission to the Special Rapporteur by the Human Rights Law Centre; and Simone Casey, "The targeted compliance framework: implications for job seekers", National Social Security Rights Network, 25 July 2019.

[68] Boris Johnson, Prime Minister, United Kingdom, statement to the General Assembly, New York, 24 September 2019.

nothing.[69] The reality is that Governments have certainly not regulated the technology industry as if human rights were at stake, and the technology sector remains a virtually human rights-free zone. The big technology companies (frequently referred to as "big tech") and their governmental supporters have worked hard to keep it that way. Their approach can be summed up for present purposes in four propositions, as set out below.

36. The first proposition is that the ability to innovate requires freedom, especially from regulation. The early call by the founder of Facebook for the industry to "move fast and break things" epitomizes the importance attached to minimizing legal and governmental constraints. However, this argument leads inexorably to a handful of powerful executives replacing Governments and legislators in determining the directions in which societies will move and the values and assumptions which will drive those developments. The accumulation of vast amounts of capital in the hands of very small elites and the rapid growth in extreme inequality have gone hand in hand with the ascendency of this approach so far.[70]

37. The second proposition is that there are no universal values. In a recent book, the President of Microsoft asked, rhetorically: "How can the world converge on a singular approach to ethics for computers when it cannot agree on philosophical issues for people?"[71] Even non-discrimination standards are sometimes presented as being too vague and contested to be useful in regulating artificial intelligence.[72] However, these arguments are self-serving and ill-informed. Governments worldwide have accepted universal human rights standards, including in the form of binding legal obligations. Over the past half century or more, these standards have been exhaustively developed and applied by courts and a wide range of expert and community-based bodies. There remains plenty of room for philosophical disagreements, but there is no absence of agreement on core human values.

38. The third proposition is that Governments are inherently slow and clumsy and tend to respond to yesterday's challenges rather than tomorrow's. The Republican minority leader of the United States House of Representatives recently argued that the bureaucratic leviathan does not have what it takes to develop or enforce nimble responses to rapid change in the technology industry.[73] While such claims might also be put forward by the proponents of unfettered discretion for the finance, aviation, defence, pharmaceutical and other industries, it is solely in relation to big tech that Governments have been prepared to abandon their regulatory responsibilities and acquiesce in a self-regulatory approach to such an extreme degree. There is no justification for such exceptionalism and no empirical evidence to support the claim that there is a fundamental incompatibility between innovation and regulation.

39. The fourth proposition is that public accountability is unnecessary because the free market is the best regulator.[74] Leaving aside the powerful arguments that big tech is deeply anti-competitive and thus immune to many currents of the free market, the great scandals of recent years that have led to the backlash against big tech (the so-called techlash) provide compelling evidence that public accountability is indispensable.

---

[69] Ibid.

[70] See Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York, Public Affairs, 2019); and Emmanuel Saez and Gabriel Zucman, *The Triumph of Injustice: How the Rich Dodge Taxes and How to Make Them Pay* (New York, W. W. Norton and Company, 2019).

[71] Brad Smith and Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (New York, Penguin Press, 2019), p. 207.

[72] Aaron Rieke, Miranda Bogen and David G. Robinson, "Public scrutiny of automated decisions: early lessons and emerging methods" (Upturn and Omidyar Network, 2018), p. 25.

[73] Kevin McCarthy, "Don't count on Government to protect your privacy", *New York Times*, 14 June 2019.

[74] See Julie Cohen, "Law for the platform economy", *U.C. Davis Law Review*, vol. 51, No. 1 (November 2017).

40. In response to growing calls for effective governmental regulation, the industry has gone into high gear in producing, influencing and embracing codes of ethics and other non-binding standards purporting to regulate digital technologies and their developers.[75] Most, but by no means all, of these codes contain a reference to human rights, but the substance of human rights law is invariably lacking. Instead, the token reference to human rights serves only to enhance claims of legitimacy and universality. Meanwhile, the relevant discussions of ethics are based on almost entirely open-ended notions that are not necessarily grounded in legal or even philosophical arguments and can be shaped to suit the needs of the industry. As a result, there are serious problems of conceptual incoherence, conflicts among norms are rarely acknowledged, meaningful input is rarely sought from stakeholders and accountability mechanisms are absent.[76] Even industry-employed ethicists acknowledge that "if ethics is simply absorbed within the logics of market fundamentalism, meritocracy, and technological solutionism, it is unlikely that the tech sector will be able to offer a meaningful response to the desire for a more just and values-driven tech ecosystem."[77] Against this background, it is unsurprising that there are few public or scholarly discussions of the human rights implications of digital welfare states.

41. The human rights community has thus far done a very poor job of persuading industry, Government or, seemingly, society at large of the fact that a technologically driven future will be disastrous if it is not guided by respect for human rights that is in turn grounded in law.

B. Ensuring legality and transparency

42. One of the most surprising characteristics of too many important digital welfare state initiatives is a lack of attention to the importance of ensuring legality. Many such examples have been drawn to the Special Rapporteur's attention, including: the online compliance intervention system of the Government of Australia, which used automated data-matching as the basis for sending out vast numbers of debt notices with very high error rates;[78] allegedly unlawful information provided to claimants over the online Universal Credit portal in the United Kingdom;[79] the contested legality of the Irish Public Services Card for some of the purposes for which it has been used;[80] the System Risk Indication system in the Netherlands, which initially

[75] These include industry standards, civil society initiatives and public frameworks. To give a few examples: IBM, "Everyday ethics for artificial intelligence" (September 2018); Google, "Artificial intelligence at Google: our principles" (2019); Microsoft, *The Future Computed* (2018); Institute of Electrical and Electronics Engineers, Global Initiative on Ethics of Autonomous and Intelligent Systems; Software and Information Industry Association, "Ethical principles for artificial intelligence and data analytics" (2017); Future of Life Institute, "Asilomar artificial intelligence principles" (2017); and Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, "Ethics guidelines for trustworthy AI" (Brussels, European Commission, April 2019).

[76] Karen Yeung, Andrew Howes and Ganna Pogrebna, "AI governance by human rights-centred design, deliberation and oversight: an end to ethics washing", in M. Dubber and F. Pasquale, eds., *The Oxford Handbook of AI Ethics* (forthcoming).

[77] Jacob Metcalf, Emanuel Moss and danah boyd [sic], "Owning ethics: corporate logics, Silicon Valley, and the institutionalization of ethics", *Social Research*, vol. 86, No. 2 (Summer 2019), p. 473.

[78] Carney, "The new digital future for welfare".

[79] Submission to the Special Rapporteur by the Child Poverty Action Group.

[80] Data Protection Commission, *Final Investigation Report: An Investigation by the Data Protection Commission in Respect of the Processing of Personal Data by the Department of Employment Affairs and Social Protection in relation to the Public Services Card ("PSC") – Examining Compliance with the Obligations in Relation to Legal Basis and Transparency* (Dublin, 2019).

lacked a legal basis and remains subject to court challenge;[81] and the Aadhaar system in India, which was originally implemented without a legal framework.[82]

43. While the lack of a legal basis is deeply problematic per se, it also means that opportunities for legislative debate and for public inputs to shape the relevant systems are also lacking. This has potentially major negative implications for transparency, design, legitimacy and the likelihood of acceptance.

C. Promoting digital equality

44. Egalitarianism is a consistent theme of the technology industry, as exemplified by Facebook's aim "to give people the power to build community and bring the world closer together".[83] At the macro level, however, big tech has been a driver of growing inequality[84] and has facilitated the creation of a "vast digital underclass".[85]

45. For its part, the digital welfare state sometimes gives beneficiaries the choice to go digital or to continue using more traditional techniques. In reality, however, policies such as "digital by default" or "digital by choice" are usually transformed into "digital only" in practice. This in turn exacerbates or creates major disparities among different groups. A lack of digital literacy leads to an inability to use basic digital tools at all, let alone effectively and efficiently. Limited or no access to the Internet poses huge problems for a great many people. Additional barriers arise for individuals who have to pay high prices to obtain Internet access, travel long distances or absent themselves from work to do so, visit public facilities such as libraries in order to get access, or obtain assistance from staff or friends to navigate the systems. Moreover, while the well-off might have instant access to up-to-date and easy-to-use computers and other hardware, as well as fast and efficient broadband speeds, the least well-off are far more likely to be severely disadvantaged by out-of-date equipment and time-consuming and unreliable digital connections.

46. In submissions to the Special Rapporteur from a wide range of countries, the salience of these different problems was emphasized. In both the global North and the global South, many individuals, especially those living in poverty, do not have a reliable Internet connection at home,[86] cannot afford such a connection,[87] are not digitally skilled or confident[88] or are otherwise inhibited from communicating with authorities online. In the various submissions, it was emphasized how those problems impede the ability of would-be claimants to realize their human rights.

---

[81] Alston, brief as amicus curiae before the District Court of the Hague on the case of *NJCM c.s./ De Staat der Nederlanden (SyRI)*.

[82] Submission to the Special Rapporteur by the Centre for Communication Governance at the National Law University, Delhi.

[83] Kevin Munger, "The rise and fall of the Palo Alto consensus", *New York Times*, 10 June 2019.

[84] Isobel Asher Hamilton, "A definitive list of the 13 richest tech billionaires in the world", *Business Insider*, 9 March 2019.

[85] Farhad Manjoo, "The tech industry is building a vast digital underclass", *New York Times*, 24 July 2019.

[86] Emily Dreyfuss, "Global Internet access is even worse than dire reports suggest", *Wired*, 23 October 2018; Organization for Economic Cooperation and Development (OECD), Internet Access database, available at https://data.oecd.org/ict/internet-access.htm; and OECD, "OECD toolkit aims to spur high-speed Internet use in Latin America and the Caribbean", 21 June 2016.

[87] Alliance for Affordable Internet, "2018 affordability report" (Washington, D.C., 2018); and World Wide Web Foundation, "New mobile broadband pricing data shows uneven progress on affordability", 21 March 2019. In the United States, 27 per cent of the population does not use high-speed broadband Internet at home, and that figure is as high as 44 per cent for people with an income below $30,000 (Pew Research Centre, "Internet/broadband fact sheet", 12 June 2019).

[88] European Commission, "Human capital: digital inclusion and skills", 2019.

47. The United Kingdom provides an example of a wealthy country in which, even in 2019, 11.9 million people (22 per cent of the population) do not have the essential digital skills needed for day-to-day life. An additional 19 per cent cannot perform fundamental tasks such as turning on a device or opening an application. In addition, 4.1 million adults (8 per cent) are offline because of fears that the Internet is an insecure environment; proportionately, almost half of those are from a low-income household and almost half are under 60 years of age.[89]

48. These problems are compounded by the fact that, when digital technologies are introduced into the welfare state, their distributive impact is often not a significant focus of Governments.[90] In addition, vulnerable individuals are not commonly involved in the development of information technology systems and information technology professionals are often ill-equipped to anticipate the sort of problems that are likely to arise.[91] It is often assumed, without justification, that individuals will have ready access to official documents and be able to upload them, that they will have a credit history or broader digital financial footprint, or even that their fingerprints will be readable, which is often not the case for those whose working lives have involved unremitting manual labour.

49. In terms of digital welfare policy, several conclusions emerge. First, there should always be a genuine, non-digital option available.[92] Second, programmes aimed at digitizing welfare arrangements should be accompanied by programmes designed to promote and teach the digital skills needed and to ensure reasonable access to the necessary equipment, as well as effective online access. Third, in order to reduce the harm caused by incorrect assumptions and mistaken design choices, digital welfare systems should be co-designed by their intended users and evaluated in a participatory manner.

D. Protecting economic and social rights in the digital welfare state

50. The processes of digitization and the increasing role played by automated decision-making through the use of algorithms and artificial intelligence have, in at least some respects, facilitated a move towards a bureaucratic process and away from one premised on the right to social security or the right to social protection. Rather than the ideal of the State being accountable to the citizen to ensure that the latter is able to enjoy an adequate standard of living, the burden of accountability has in many ways been reversed. To a greater degree than has often been the case in the past, today's digital welfare state is often underpinned by the starting assumption that individuals are not rights holders but rather applicants. In that capacity, people must convince the decision-makers that they are deserving, that they satisfy the eligibility criteria, that they have fulfilled the often onerous obligations prescribed and that they have no other means of subsistence. In addition, much of this must be done electronically, regardless of applicants' skills in that domain.

[89] "The digitally disadvantaged", in Lloyds Bank, *UK Consumer Digital Index 2019 – Key Findings* (London, 2019).

[90] Mary Madden, "The devastating consequences of being poor in the digital age", *New York Times*, 25 April 2019.

[91] Submission to the Special Rapporteur by Norbert Jansen (ICTU, the Netherlands).

[92] Submissions to the Special Rapporteur by the Association for Progressive Communications, Derechos Digitales and Media Matters for Democracy; Citizens Advice Scotland; and the National Social Security Rights Network.

51. The right to social security[93] encompasses the right to access and maintain benefits, whether in cash or in kind, without discrimination.[94] The imposition of technological requirements can make it impossible or very difficult for individuals to effectively access that right.[95]

52. The right to social protection is integrally linked to what the Human Rights Committee refers to as the right to life with dignity, which must be protected, where necessary, through measures designed to ensure access without delay by individuals to essential goods and services such as food, water, shelter, health care, electricity and sanitation, and other measures designed to promote and facilitate adequate general conditions.[96] Various other rights are also implicated, including the right to an adequate standard of living, the right to mental health and the right to be treated with dignity.

53. While social protection in general should be designed to protect those rights, the dignity dimension is at particular risk in the context of the digital welfare state. The potential risks arise in various contexts.

54. First, the process for determining eligibility may easily be transformed into an electronic question-and-answer process that almost inevitably puts already vulnerable individuals at even greater disadvantage.

55. Second, the way in which determinations are framed and communicated may be dehumanized and allow no room for meaningful questioning or clarification.

56. Third, the digital welfare state often seems to involve various forms of rigidity and the robotic application of rules. As a result, extenuating circumstances, such as being late for an appointment because of urgent caring obligations or being unable to understand a written communication because of a disability or a personal crisis, are often not taken into account in a predominantly digital context.

57. Fourth, digital systems are often not designed to respond rapidly either to serious emergencies or to daily challenges, such as those that may be experienced by an older person whose entitlement has suddenly and inexplicably been electronically reduced or cancelled or by a single parent unable to take a child to a local day care because the digital identification card will not function.

58. Fifth, the ways in which services are provided can easily have degrading connotations, such as unnecessarily exposure to a broader audience the fact that a person is reliant on benefits, or requiring extended waiting periods or the navigation of lengthy queues.

59. Sixth, the introduction of various new technologies that eliminate the human provider can enhance efficiency and provide other advantages but might not necessarily be satisfactory for individuals who are in situations of particular vulnerability. New technologies often operate on the law of averages, in the interests of majorities and on the basis of predicted outcomes or likelihoods.

60. Seventh, digital services risk eliminating, almost entirely, much of the human interaction and compassion that are likely to be indispensable components in providing at least some welfare recipients with the care and assistance they need. The assumption that there is always a technological fix for any problem is highly likely to be misplaced in various aspects of a humane and effective system of social protection.

[93] International Covenant on Economic, Social and Cultural Rights, art. 9.

[94] Committee on Economic, Social and Cultural Rights, general comment No. 19 (2007) on the right to social security, para. 2.

[95] Ibid, paras. 24–27.

[96] Human Rights Committee, general comment No. 36 (2018) on the right to life, para. 26.

E. Protecting civil and political rights in the digital welfare state

61. That the poor suffer from more intense levels of scrutiny, monitoring and surveillance is hardly an original observation. In the 1960s, Charles Reich wrote that welfare recipients in the United States had been subjected to many forms of procedure and control not imposed on other citizens and were all too easily regulated.[97] In 1975, Michel Foucault wrote about the "coercive technologies of behaviour" used in modern society to discipline and punish the poorer classes.[98]

62. By way of explaining why these lessons have not been learned in the digital welfare state, Shoshana Zuboff writes that the system of "surveillance capitalism" that prevails today is unprecedented, which has enabled it to elude systematic contest because it cannot be adequately grasped with our existing concepts.[99] This private surveillance is being reinforced by trends in government surveillance. Jack Balkin has described the "national surveillance state" as a permanent feature of governance that will become as ubiquitous in time as the familiar devices of the regulatory and welfare states.[100]

63. Digital technologies are employed in the welfare state to surveil, target, harass and punish beneficiaries, especially the poorest and most vulnerable among them. Once again, many of the submissions received by the Special Rapporteur serve to illustrate and reinforce this point. A number of human rights concerns are highlighted in them.

64. A first concern, in the context of social security benefits and assistance, is that there is a real risk of beneficiaries being effectively forced to give up their right to privacy and data protection to receive their right to social security, as well as other social rights.[101]

65. A second concern is the blurring of the lines between public and private surveillance. Welfare state authorities increasingly rely, either actively or passively, on private corporations for the surveillance and targeting of beneficiaries. Private entities have different motives for their involvement in benefit and social assistance systems and this may lead to conflicts between the public interests that these systems ought to serve and the private interests of corporations and their owners.

66. A third concern is the potential for deliberate targeting and harassment of the poor through new technologies in the welfare state. As highlighted in one submission to the Special Rapporteur, fraud in the welfare state is often the result of confusion, complexity and the inability to correct the resulting errors.[102] However, by deliberately using the power of new technologies to identify fraud or violations of "conditionalities" imposed on beneficiaries, Governments are likely to find inconsistencies that they can hold against claimants. It is relevant here that new technologies are enabling what Jack Balkin described as the "death of amnesia": new abilities to collect information and store it digitally for an undefined period of time create a future in which a wealth of information can be held against someone indefinitely.[103]

---

[97] Charles A. Reich, "Individual rights and social welfare: the emerging legal issues", *Yale Law Journal*, vol. 74, No. 7 (1965), p. 1245.

[98] Foucault, *Discipline and Punish*, p. 222.

[99] Zuboff, *The Age of Surveillance Capitalism*, p. 14.

[100] Jack M. Balkin, "The constitution in the national surveillance state", *Minnesota Law Review* (vol. 93, No. 1 (2008)).

[101] Submission to the Special Rapporteur by the Government of Mexico; and Philip Alston, Special Rapporteur on extreme poverty and human rights, statement on visit to the United States, 15 December 2017, para. 57.

[102] Submission to the Special Rapporteur by Norbert Jansen (ICTU, the Netherlands).

[103] Balkin, "The constitution in the national surveillance state", p. 13.

67. Additional concerns that warrant greater consideration than can be provided in the present report include: (a) the human rights consequences of the move to predicting risk instead of the ex post enforcement of rules violations;[104] (b) the dangers of connecting Government data silos, which is more readily contemplated in the welfare context than elsewhere in the field of digital governance;[105] (c) the psychological and societal cost of constant monitoring and surveillance;[106] and (d) the growing tendency of some Governments to use the opportunities provided by the digital welfare state to try to alter social behaviours, such as sexual activity or preferences, approaches to cohabitation, the use of alcohol or drugs and the decision to have children.[107]

F. Resisting the inevitability of a digital-only future

68. Digital technologies in general, and especially those central to the digital welfare state, are often presented as being both unavoidable and irresistible. If a country wants to be seen to be at the technological cutting edge, if its Government wants to have the most efficient, economical and flexible welfare system available and if its citizenry wants all of the convenience that comes from not having to provide identification in order to undertake various transactions, then a transition to a digital welfare state must be pursued. However, quite apart from the choices that citizens and Governments might make if they were fully informed and adequately consulted, the reality is that such decisions are all too often taken in the absence of sophisticated cost-benefit analyses. When such analyses are undertaken, they consist of financial balance sheets that ignore what might be termed the fiscally invisible intangibles that underpin human rights. Values such as dignity, choice, self-respect, autonomy, self-determination and privacy are all traded off without being factored into the overall equation, all but guaranteeing that insufficient steps will be taken to ensure their role in the new digital systems.

69. It is often assumed that at least some of these trade-offs can be justified on the grounds that the bargain is just a matter between the individual and a particular government agency. However, such an image is increasingly very far from the truth as cross-matching, data-sharing and cross-verification systematically enlarge the pools of data potentially available across the spectrum of governance. To the extent that assurances are given that leakage from one silo to the next will not occur, such guarantees are largely illusory as a change of Government or a real or imagined emergency situation is all that is required to trigger a partial or comprehensive breaking down of the partitions, quite apart from the risks of electronic data breaches resulting from hacking or normal system breakdowns. In addition, the assumption that the relationship is only between Government and citizen is also anachronistic. Corporate actors now play a central role in large parts of the welfare system and, when taken together with the ever-expanding reach of other forms of surveillance capitalism, intangible human rights values can be assumed to be worth as much as the shares of a bankrupt corporation.

[104] Ibid., p. 11.

[105] Reetika Khera, “These digital IDs have cost people their privacy – and their lives”, *Washington Post*, 9 August 2018.

[106] Research with civil society groups has shown that concerns about stigmatization and feelings of being targeted are more prominent than privacy concerns per se (submission to the Special Rapporteur by the Data Justice Lab at Cardiff University).

[107] See Foucault’s analysis of panoptic systems that could be used as a machine to carry out experiments, to alter behaviour, to train and correct individuals (Foucault, *Discipline and Punish*, p. 203).

70. The Special Rapporteur has learned of situations in which crucial decisions to go digital have been taken by government ministers without consultation, or even by departmental officials without any significant policy discussions taking place, on the grounds that the move is essentially an administrative matter, rather than one involving a potentially game-changing approach to a large swathe of official policy. Sometimes, there seems to be a presumption that, even if the move to digital is not currently necessary, it surely will be one day and it is better to move in advance. Support for such pre-emptive moves may come from corporate interests, as well as from the security and counter-terrorism sectors, albeit for quite different reasons. Careful and transparent consideration should always be given to the questions of why, for whom, when and how transitions to digital systems take place.

71. Even where detailed cost estimates are provided, accuracy seems difficult to achieve. Helen Margetts has observed that, in the United Kingdom, for example, technology and the public sector have rarely been happy bedfellows and every government technology project seems doomed to arrive late, underperform and come in over budget.[108] Another example is the Aadhaar system in India, which is said to have lacked a proper cost-benefit analysis prior to implementation[109] and in relation to which there has been great disagreement as to the post hoc assessment of costs and benefits.[110]

G. Role of the private sector

72. Two consistent themes of the present report have been the reluctance of many Governments to regulate the activities of technology companies and the strong resistance of those companies to taking any systematic account of human rights considerations. The fact that this leads to many large technology corporations operating in an almost human rights-free zone is further exacerbated by the extent to which the private sector is taking a leading role in designing, constructing and even operating significant parts of the digital welfare state.[111]

73. Among well-known examples are the involvement of the Net1 subsidiary Cash Paymaster Services, MasterCard and Grindrod Bank in the distribution of social grants linked to the biometric identification system of South Africa, the roles played by Indue and Visa in the cashless debit card trials in Australia and the involvement of IBM in the Social Assistance Management System in Ontario, Canada. In submissions to the Special Rapporteur, attention was also drawn to the increasing role of the private sector in Germany for public administration software used for unemployment services and social and youth welfare;[112] and outsourcing by local authorities in the United Kingdom to private companies in the area of social protection.[113] In contrast,

[108] Helen Margetts, “Back to the bad old days, as civil service infighting threatens United Kingdom’s only hope for digital government”, The Conversation, 9 August 2016.

[109] Submission to the Special Rapporteur by the Centre for Communication Governance at the National Law University, Delhi.

[110] Reetika Khera, “A ‘cost-benefit’ analysis of UID”, *Economic and Political Weekly*, vol. 48, No. 5 (February, 2013); Kieran Clarke, “Estimating the impact of India’s Aadhaar scheme on liquid petroleum gas subsidy expenditure”, International Institute for Sustainable Development, 16 March 2016; Jean Drèze and Reetika Khera, “Aadhar’s $11-billion question”, *Economic Times*, blog, 17 February 2018; Anand Venkatanarayanan, “The curious case of the World Bank and Aadhaar savings”, The Wire, 3 October 2017; and Aria Thaker, “Emails from a World Bank official reveal why India shouldn’t brag about $11 billion Aadhaar savings”, Quartz India, 10 January 2019.

[111] Submissions to the Special Rapporteur by the Government of Croatia, the Government of Estonia and the Government of Ireland.

[112] Submissions to the Special Rapporteur by AlgorithmWatch.

[113] Submission to the Special Rapporteur by the Data Justice Lab at Cardiff University.

the deliberate choice by some Governments not to rely on private actors to play key roles in the welfare state was pointed out in some submissions.[114]

74. The Special Rapporteur has addressed elsewhere the issues arising out of the privatization of public services more generally (A/73/396). However, in relation to social protection services, there is a deeply problematic lack of information about the precise role and responsibility of private actors in proposing, developing and operating digital technologies in welfare states around the world. This lack of transparency has a range of causes, from gaps in freedom of information laws, confidentiality clauses and intellectual property protections to a failure on the part of legislatures and executives to require transparency and a general lack of investigation of these practices by oversight bodies and the media.[115] The absence of information seriously impedes efforts to hold Governments and private actors accountable.

H. Accountability mechanisms

75. Many of the programmes used to promote the digital welfare state have been designed by the very same companies that are so deeply resistant to abiding by human rights standards. Moreover, those companies and their affiliates are increasingly relied upon to design and implement key parts of the welfare programmes themselves. It is thus evident that the starting point for efforts to ensure human rights-compatible digital welfare state outcomes is to ensure, through governmental regulation, that technology companies are legally required to respect applicable international human rights standards.[116]

IV. Conclusions

76. **There is no shortage of analyses warning of the dangers for human rights of various manifestations of digital technology and, especially, artificial intelligence. However, these studies are overwhelmingly focused on traditional civil and political rights such as the right to privacy, non-discrimination, a fair trial and freedom of expression and information. Few studies have adequately captured the full array of threats represented by the emergence of the digital welfare state. The vast majority of States spend very large amounts of money on different forms of social protection, or welfare, and the allure of digital systems that offer major cost savings along with personnel reductions, greater efficiency and fraud reduction, not to mention the kudos associated with being at the technological cutting edge, is irresistible. There is little doubt that the future of welfare will be integrally linked to digitization and the application of artificial intelligence.**

77. **However, as humankind moves, perhaps inexorably, towards the digital welfare future, it needs to alter course significantly and rapidly to avoid stumbling, zombie-like, into a digital welfare dystopia. Such a future would be one in which unrestricted data-matching is used to expose and punish the**

[114] Submissions to the Special Rapporteur by the Government of Argentina, the Government of Greece and Louise Humpage (University of Auckland).

[115] Submissions to the Special Rapporteur by AlgorithmWatch, Privacy International and the Irish Council for Civil Liberties.

[116] See Yeung, Howes and Pogrebna, "Artificial intelligence governance by human rights-centred design"; Paul Nemitz, "Constitutional democracy and technology in the age of artificial intelligence", *Philosophical Transactions A*, vol. 376, No. 2133 (2018); and Karen Yeung, *A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework*, MSI-AUT(2018)05 rev (Council of Europe, 22 May 2019).

slightest irregularities in the record of welfare beneficiaries (while assiduously avoiding such measures in relation to the well-off); evermore refined surveillance options enable around-the-clock monitoring of beneficiaries; conditions are imposed on recipients that undermine individual autonomy and choice in relation to sexual and reproductive choices and choices in relation to food, alcohol, drugs and much else; and highly punitive sanctions are able to be imposed on those who step out of line.

78. **It will be argued that the present report is unbalanced, or one-sided, because the dominant focus is on the risks rather than on the many advantages potentially flowing from the digital welfare state. The justification is simple. There are a great many cheerleaders extolling the benefits, but all too few counselling sober reflection on the downsides. Rather than seeking to summarize the analysis above, a number of additional observations are in order.**

79. **First, digital welfare state technologies are not the inevitable result of scientific progress, but instead reflect political choices made by humans. Assuming that technology reflects preordained or objectively rational and efficient outcomes risks abandoning human rights principles along with democratic decision-making.**

80. **Second, if the logic of the market is consistently permitted to prevail, it inevitably disregards human rights considerations and imposes externalities on society, for example when artificial intelligence systems engage in bias and discrimination and increasingly reduce human autonomy.**[117]

81. **Third, the values underpinning and shaping the new technologies are unavoidably skewed by the fact that there is a diversity crisis in the artificial intelligence sector across gender and race.** [118] **Those designing artificial intelligence systems in general, as well as those focused on the welfare state, are overwhelmingly white, male, well-off and from the global North. No matter how committed they might be to certain values, the assumptions and choices made in shaping the digital welfare state will reflect certain perspectives and life experiences. The way to counteract these biases and to ensure that human rights considerations are adequately taken into account is to ensure that the practices underlying the creation, auditing and maintenance of data are subjected to very careful scrutiny.**[119]

82. **Fourth, predictive analytics, algorithms and other forms of artificial intelligence are highly likely to reproduce and exacerbate biases reflected in existing data and policies. In-built forms of discrimination can fatally undermine the right to social protection for key groups and individuals. There therefore needs to be a concerted effort to identify and counteract such biases in designing the digital welfare state. This in turn requires transparency and broad-based inputs into policymaking processes. The public, and especially those directly affected by the welfare system, need to be able to understand and evaluate the policies that are buried deep within the algorithms.**

---

[117] Anton Korinek, "Integrating ethical values and economic value to steer progress in artificial intelligence", National Bureau of Economic Research Working Paper, No. 26130 (Cambridge, Massachusetts, 2019), p. 2.

[118] Women make up 15 per cent of artificial intelligence research staff at Facebook and 10 per cent at Google; only 2.5 per cent of Google's workforce is black, while Facebook and Microsoft are each at 4 per cent (Sarah West, Meredith Whittaker and Kate Crawford, "Discriminating systems: gender, race and power in AI" (AI Now Institute, 2019)).

[119] Rashida Richardson, Jason M. Schultz, and Kate Crawford, "Dirty data, bad predictions: how civil rights violations impact police data, predictive policing systems, and justice", *New York University Law Review* (May 2019).

83. **Fifth, especially, but not only, in the Global North, the technology industry is heavily oriented towards designing and selling gadgets for the well-off, such as driverless and flying cars and electronic personal assistants for multitasking businesspeople. In the absence of fiscal incentives, government regulation and political pressures, it will devote all too little attention to facilitating the creation of a welfare state that takes full account of the humanity and concerns of the less well-off in any society.**

84. **Sixth, to date, astonishingly little attention has been paid to the ways in which new technologies might transform the welfare state for the better. Instead of obsessing about fraud, cost savings, sanctions and market-driven definitions of efficiency, the starting point should be how existing or even expanded welfare budgets could be transformed through technology to ensure a higher standard of living for the vulnerable and disadvantaged and to devise new ways of caring for those who have been left behind and more effective techniques for addressing the needs of those who are struggling to enter or re-enter the labour market. That would be the real digital welfare state revolution.**