**Check against delivery**

# Statement by Philip Alston
# SPECIAL RAPPORTEUR ON EXTREME POVERTY AND HUMAN RIGHTS

74th session of the General Assembly
Third Committee
Item 70 (c)

18 October 2019
New York

**Statement by Professor Philip Alston, Special Rapporteur on extreme poverty and human rights**

Mr Chairperson, distinguished delegates,

My mandate as Special Rapporteur comes to an end on April 30, 2020. Accordingly, this is the final report that I will present in person to either the General Assembly's Third Committee or to the UN Human Rights Council. Before addressing the substance of my report to the current session of the General Assembly, I would like to take a moment to express my deep appreciation to those who have worked with me on this mandate, some of whom have been indispensable partners on this journey. It is an oddity or idiosyncrasy of the UN system that those who so often do the real work must go unthanked in the name of some anachronistic sense of the need for anonymity.

I would like to thank several officials of the OHCHR, and they know who they are, for the invaluable assistance they provided to the mandate. In addition, there is one official in particular who has worked with me for almost the entire period of my mandate and has shown extraordinary knowledge, dedication, initiative, and above all wisdom. I understand that the unwritten rules prevent me from naming her, but I owe her a huge debt and she deserves great credit for whatever has been accomplished over the past almost six years. Then there are those who I can name, because they were my collaborators at New York University, and they too have made an immense contribution. First and foremost, I thank Christiaan van Veen who has been my trusted adviser from the beginning and is now directing an important project on the digital welfare state and human rights, based at NYU Law School. I also want to thank Rebecca Riddell and Bassam Khawaja, who are true professionals in the best sense of the word, and Anna Bulman whose assistance was greatly appreciated. Finally I must say that nothing I did in relation to this mandate would have been possible without the sage advice and unflagging support of Professor Gráinne de Búrca.

Mr Chairperson,

The report that I am presenting today focuses on the intersection of a number of key recent developments. The background consists of three elements.

- the era of digital governance means that the majority of Governments around the world are moving to digitize many of their systems.
- this almost invariably involves the development of national identity systems, many of which capture comprehensive biometric data. $18b was spent worldwide on this last year. In five years from now, that figure will be three times higher.
- the justifications offered for the adoption of what are actually or potentially extraordinarily intrusive and far-reaching surveillance systems usually focus on the enhancement of social protection or the welfare state, along with improving government efficiency, and rooting out fraud.

Against this background, I want to flag a number of concerns.

First, the digital welfare state is commonly presented as an altruistic and noble enterprise designed to ensure that citizens benefit from new technologies, experience more efficient government, and enjoy higher levels of well-being. Systems of social protection and assistance are increasingly driven by digital data and technologies that are used for diverse purposes, including to automate, predict, identify, surveil, detect, target and punish. But the very real risk is that we are 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 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 in relation to food, alcohol and drugs and much else; and highly punitive sanctions are able to be imposed on those who step out of line.

Second, digital welfare states thereby risk becoming a Trojan Horses for neoliberal hostility towards social protection and regulation. The digitization of welfare systems has very often been used to promote 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.

Third, many of the Governments that are moving at breakneck speed to introduce these digital biometric ID systems are behaving like the Queen in Alice in Wonderland: "digital system first, law later". In other words, little thought is being given to the sorts of legal bases for these developments and more importantly to the various protections that are essential to prevent future disasters of various kinds. Take security as just one example. The risks flowing from the existence of these huge, all-seeing, databases come from many directions: (i) misuse by the government, or by constituent parts thereof; (ii) politically-motivated manipulation or abuse of the system; (iii) extensive and deep private sector access without adequate safeguards; and (iv) hacking, or the huge risks that security will be compromised, potentially on a massive scale.

Fourth, there are examples from around the world of situations in which governments have failed to think through carefully and then to spell out the goals and objectives of these massive undertakings. Again there is the sense that the spirit is to get the system in place first and then we'll work out what we might use it for. A better recipe for abuse is difficult to imagine.

Fifth, the private sector is often a driving force for the adoption of these systems. The private sector sells the idea, designs the software and the algorithms, implements the programs, provides the hardware, distributes the benefits and social protection, and much more. Yet this is the same private sector that is, by its own insistence and design, not committed to or governed by human rights standards. Weak codes of ethics that make a fleeting token reference to human rights and then rely on the subjective preferences of Big Tech offer no protection for the rights and interests of individuals.

Sixth, the decisions to adopt and implement these biometric ID systems and the related digital welfare systems pose a major threat to democracy, since they are all too rarely the subject of serious public debate and scrutiny. Instead they are presented as essentially administrative or technical innovations to be approved by ministers or even just by unelected officials. But in fact the potential implications for democracy and for human rights more generally are potentially immense. Transparency and accountability are consistent casualties of the way in which these systems are being adopted.

Seventh, the human rights community, broadly defined, is too often looking in the wrong direction when it comes to these developments. There is no shortage of analyses warning of the dangers for human rights of various manifestations of digital technology and especially artificial intelligence. But these studies focus overwhelmingly on the traditional civil and political rights such as the right to privacy, non-discrimination, fair trial rights, and the right to freedom of expression and information. With a handful of exceptions, none has 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 AI.

Eighth, problems of discrimination and bias are endemic in this area. The values underpinning and shaping the new technologies are unavoidably skewed by the fact that there is "a diversity crisis in the AI sector across gender and race". Those designing AI 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.

Finally, and in some ways most importantly, 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 on how existing or even expanded welfare budgets could be transformed through technology to ensure a higher standard of living for the vulnerable and disadvantaged, 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.