JUDICIAL REVIEW
2020, VOL. 25, NO. 1, 39–45
https://doi.org/10.1080/10854681.2020.1732742

Routledge
Taylor & Francis Group

Public Law, the Digital World and Human Rights: Challenges Ahead

Kate O'Regan*

Bonavero Institute of Human Rights, University of Oxford

1. It is only 19 years ago since Kofi Annan, then Secretary General of the United Nations, claimed that we were living in 'The Age of Human Rights'.[1] The preceding decade had seen the fall of the Berlin Wall and a remarkable growth in the number of democracies that entrenched human rights. My own country, South Africa, was one of those that adopted a new Constitution following the transition to democracy in the mid-1990s, which entrenched a generous Bill of Rights at its heart. Kofi Annan's claim that we were living 'The Age of Human Rights' thus seemed quite fitting. Yet the last decade has seen worrying developments that suggest that "The Age of Human Rights" might already be ending.

2. In its most recent *Freedom in the World* report, Freedom House concludes that 2018 was the thirteenth consecutive year of decline in global freedom. The trend was observed in all the regions of the world, in established democracies like the United States and in consolidated authoritarian regimes like Russia and China. Countries previously hovering on the borderline of authoritarianism have "shed the thin façade of democratic practice" of previous decades, when international incentives for reform were stronger.[2] The status of 19 countries declined in 2018, with the sharpest declines occurring in Nicaragua, Tanzania, Venezuela and Serbia. Just six countries countered the trend, including Malaysia, Ethiopia, Armenia and Ecuador.

3. Freedom House identifies several recurrent manifestations of this decline, including: (a) the weakening commitment to free and fair elections, as nations "find ways to control their results while sustaining a veneer of competitive balloting";[3] (b) the overturning of presidential or executive term limits, including the decision by China's National People's Congress in 2018 to remove the two-term limit on the presidency;[4] (c) a range of assaults on freedom of expression, including the imprisonment of journalists such as

*Professor of Human Rights Law and Director of the Bonavero Institute of Human Rights, University of Oxford; Judge, Constitutional Court of South Africa (1994–2009).

[1]Kofi A. Annan, "The Age of Human Rights" (Project Syndicate, 26 September 2000) <www.project-syndicate.org/commentary/the-age-of-human-rights> (accessed 16 December 2019).

[2]Freedom House, *Freedom in the World 2019* (2019), p. 1 <https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf> (accessed 16 December 2019).

[3]Ibid. p. 4.

[4]There have been 34 attempts to revise presidential or executive term limits over the last 13 years, of which 31 have been successful. See ibid. pp. 4–5, 9.

Wa Lone and Kyaw Soe Oo in Myanmar, the appalling murder of Jamal Khashoggi in Istanbul in 2018, and a rise in prosecutions for criticism of politicians;[5] and (d) a disturbing increase in forms of ethnic cleansing in countries such as Syria, Myanmar, Russia and China.[6]

4. Many of these authoritarian and illiberal practices are based on the use or abuse of technology. Key examples include censorship of online content, surveillance using a range of technologies, including artificial intelligence (AI) and facial recognition, and blanket shutdowns of the internet and communications networks during times of political turmoil.

5. China leads the world in the authoritarian and illiberal use of technology.[7] In 2017, China adopted a new cybersecurity law that increased censorship requirements, mandated data localisation, codified real-name registration requirements for internet companies and obliged them to assist security services with investigations. Both Chinese and foreign internet companies are compelled to comply with this invasive legislation.

6. China has also embraced surveillance technology, including AI, facial recognition and intrusive surveillance apps. Coupled with police access to user data, these technologies have dramatically increased surveillance and have led to the prosecution of prominent dissidents, amongst others.

7. At the Communist Party Congress in October 2017, President Xi Jinping announced plans to turn China into a cyber superpower and to offer its authoritarian model of governance "as a new option for other countries and nations that want to speed up their development".[8] China has held training or seminars for 36 countries on cyber surveillance during the last year.[9]

8. But China is most certainly not alone. In India, the controversial rollout of the Aadhaar system of biometric identification has led to deep-seated anxiety that it may be used for illiberal purposes. The system is aimed at authenticating the identities of individuals who apply for services both from government and the private sector. Services that require Aadhaar authentication include opening bank accounts, obtaining mobile SIM cards, paying income tax and accessing government services. To enrol in the Aadhaar system, an individual must provide their fingerprints, iris biometric information, and demographic details, all of which are stored on a central database. Whenever an individual applies for a service, their identity is checked against the central database, and the application for authentication may be stored. When Aadhaar was

[5]In Turkey, for example, 2017 saw more than 20,000 investigations and 6,000 prosecutions for 'insulting the President'. See ibid. pp. 5–6.
[6]Ibid. p. 7.
[7]See Adrian Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism* (Freedom House, 2018) <https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf> (accessed 16 December 2019).
[8]Ibid. p. 7.
[9]Ibid. p. 2.

originally introduced in 2010, it was described as a voluntary scheme, but participation is now effectively mandatory. A major constitutional challenge to Aadhaar was heard by the Supreme Court of India in 2017 and 2018.[10] The challenge concerned the system's regulatory framework, design, and effect on individual rights. The petitioners argued that:

> by building a nationwide centralised biometric database, and by giving itself the power to track people's daily transactions every time they were required to authenticate themselves, the state was distorting the balance of power that was at the heart of the constitutional order and threatening freedom.[11]

9. After a marathon hearing lasting 38 days, the Supreme Court, by a majority of four to one, upheld the overall constitutionality of the system, although it struck down some of its important elements.

10. India provides other examples of the link between technology and authoritarianism. In August 2019, following its revocation of the special status of Jammu and Kashmir under Art. 370 of the Indian Constitution, the Indian Government instituted a lengthy shutdown of internet and phone services in the region. This is not the first such shutdown in Jammu and Kashmir. In 2016, after the killing of a separatist leader, Burham Wani, mobile and landline telephone services were suspended, cable TV blocked and newspapers shut, in some cases for more than 200 days.[12]

11. Internet shutdowns are an increasingly popular authoritarian tool. According to Access Now, an international non-governmental organisation, the number of internet shutdowns worldwide has risen from 75 in 2016, to 106 in 2017, and 196 in 2018. The vast majority of the 2018 shutdowns occurred in India (134), but a range of other countries implemented them, including Pakistan (12), Yemen (7), Iraq (7), Ethiopia (6), Bangladesh (5), Russia (2), the Philippines (2) and Chad (2).[13]

12. From within the UK, it might be tempting to dismiss the decline in freedom and the rise in the illiberal and authoritarian use of technology as problems only for other states. But that would be unwise for two reasons.

13. First, the digital and technological revolutions are altering the relationship between the state, individuals and corporations in ways that we do not yet fully understand. Our current understanding of the relationship between the state and individuals is built on normative and human rights principles developed in the pre-digital world.

[10] *Justice K S Puttaswamy v Union of India* 2018 SCC Online SC 1642.
[11] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* (HarperCollins, 2019).
[12] See Daniela Flamini, "The scary trend of internet shutdowns" (Poynter, 1 August 2019) <https://www.poynter.org/reporting-editing/2019/the-scary-trend-of-internet-shutdowns> (accessed 16 December 2019).
[13] Access Now, "The state of internet shutdowns" (Access Now, 8 July 2019) <https://www.accessnow.org/the-state-of-internet-shutdowns-in-2018/> (accessed 16 December 2019).

It is not clear how easily those principles can be applied to the digital world. What is clear is that we are already in a game of catch up. The technological revolution has been rapid, and our normative toolkit must develop in response. Technology has much to offer and might well help solve persistent governance problems. But ensuring that technology operates consistently with fundamental rights is not an easy task. I briefly consider three important issues relating to the digital world that are currently under consideration in the UK to illustrate how important it is that we recognise that the digital and technological revolution is affecting many aspects of our world that need to be evaluated employing a human rights framework: online courts and tribunals, automated decision-making, and the regulation of social media

14. The UK government is in the midst of a dramatic programme to digitise and automate much of the court and tribunal system.[14] Academics, practitioners and civil society organisations must scrutinise this programme closely, to ensure that new technologies do in fact address longstanding problems, rather than exacerbating existing patterns of exclusion or introducing new ones. During both design and implementation, researchers must have access to data and information sufficient to analyse and assess the impact of the new system.

15. Second, automated decision-making and algorithms now play a role in almost every area of our lives. As Virginia Eubanks has recently noted:

> Forty years ago nearly all of the major decisions that shape our lives – whether or not we are offered employment, a mortgage, insurance, credit or a government service – were made by human beings. … Today, we have ceded much of that decision-making power to sophisticated machines. Automated eligibility systems, ranking algorithms and predictive risk models control which neighbourhoods get policed, which families attain needed resources, who is short-listed for employment and who is investigated for fraud. … Digital security guards collect information about us, make inferences about our behaviour and control access to resources.[15]

16. It is well established that algorithms often reproduce and at times aggravate patterns of bias and discrimination in decision-making. Here too, we require the conceptual and practical tools to scrutinise automated systems and to foster algorithmic decision-making that is free of bias and discrimination.

17. Finally, the regulation of social media is one of the most pressing issues at the intersection of public law and technology. While there is a growing conversation about this challenge, the best way forward remains unclear. In April 2019, the UK government published its *Online Harms White Paper*, which proposed an ambitious and far-reaching framework for the regulation of digital media.[16] One of the key recommendations is a

[14]See generally Ministry of Justice, *Transforming Our Justice System* (2016); Joshua Rozenberg, "The Online Court: Will IT Work?" (2017) <https://long-reads.thelegaleducationfoundation.org/> (accessed 16 December 2019).
[15]Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor* (St Martin's Press, 2017), p. 5.
[16]Department for Digital, Media, Culture and Sport and Home Office, *Online Harms White Paper* (April 2019).

statutory duty of care owed by all companies and institutions that own or manage websites which host or facilitate the sharing or discovery of user-generated content. The contours of the duty of care, it is proposed, will be provided by Codes of Conduct yet to be developed, but the overall purpose is to require website owners and managers to take reasonable steps to ensure their users are safe and to tackle illegal and harmful activity. The duty of care will be enforced by a regulator, rather than giving rise to a private cause of action.

18. The White Paper is one of a growing number of proposals around the world for the regulation of social media. Another notable example is the German Network Enforcement Law, or Netzgesetz, which came into force at the beginning of 2018. The Netzgesetz covers a far narrower field of services and platforms than the scheme proposed by the White Paper, and regulates a narrower array of harms, focussing only on content that is unlawful under the German Criminal Code. The Netzgesetz requires large social media platforms to introduce effective complaints systems and to undertake to remove unlawful content speedily. One of the concerns about the system is the lack of clarity over the types of content that must be removed from platforms. The system does not require any public audit of the complaints system. As with the justice system reform programme and the spread of algorithmic decision-making, assessing the human rights impact of the Netzgesetz requires a detailed study of its actual operation in practice. So far that has not been undertaken. Whether it is possible to effectively prevent online harms while protecting freedom of expression and privacy remains to be seen.[17]

19. These are just two examples that illustrate how technological developments must be regulated to protect fundamental rights. There are many others, such as the regulation of online political advertising and the problem of misinformation, which also require attention. Addressing these challenges will require substantial and sustained work at both the normative and the policy levels to develop the use of technologies in a manner that is respectful of rights, as well as research to determine whether these technologies, when implemented, indeed function in a way that is respectful of rights.

20. A second and entirely different reason for concern about the illiberal and authoritarian use of technology is the growing support around the world for an emerging illiberal and authoritarian politics. One of the striking aspects of the global rise of authoritarianism is how it seems to differ from patterns of authoritarianism in the second half of the twentieth century. When the Portuguese Carnation Revolution occurred in 1974, marking the commencement of what Samuel P. Huntington called the "third wave of democracy",[18] only 30 per cent of the world's countries (46) were electoral

[17]See generally Jacob Rowbottom, "Introduction: Symposium Online Harms White Paper" (2019) 11 *Journal of Media Law* 1; Lorna Woods, "The Duty of Care in the Online Harms White Paper" (2019) 11 *Journal of Media Law* 6; Stefan Theil, "The Online Harms White Paper: Comparing the UK and German Approaches to Regulation" (2019) 11 *Journal of Media Law* 41.
[18]Samuel P. Huntington, *The Third Wave: Democratization in the Late Twentieth Century* (University of Oklahoma Press, 1991).

democracies in which voters could choose their government in free, fair and regular elections.[19] Most of those were the liberal democracies of the rich West, with only a handful from the rest of the world: India, Sri Lanka, Costa Rica, Colombia, Venezuela and Turkey. That situation changed dramatically over the next three decades. By 2005, 60 per cent of the countries of the world were electoral democracies. But since then, as discussed above, those steady improvements in freedom and democracy have begun to fall away. Much of that recent reversal has not been the abrupt result of a military coup or a foreign invasion, as was often the case in the twentieth century, but rather a pattern of what has been called democratic erosion or democratic decay. Many countries have "experienced significant erosions in electoral fairness, political pluralism, and civic space for opposition and dissent, typically as a result of abusive executives intent upon concentrating their personal power and entrenching ruling-party hegemony".[20]

21. In many of the countries experiencing democratic decay, we see an emerging politics with shared characteristics. First, this emerging politics is often built on a distrust of political elites, which leads to attacks on traditional constitutional checks and balances, such as the judiciary and even parliament, but also other institutions of liberal democracy, such as the independent media, civil society organisations and universities. The result is invariably an executive with enhanced power over the other branches of government. Second, this politics attacks individual rights, including freedom of speech and association, and freedom from discrimination on grounds of race, religion, gender and LGBTI status. Third, this emerging politics is, perhaps surprisingly, largely waged in cultural and identitarian terms, rather than in terms of distributive or economic justice.

22. Elements of this emerging politics can be found in many contemporary democracies. In Europe, the clear examples are Hungary and Poland, but many political parties on the continent make similar claims. They can also be found in India, Brazil, the Philippines, Turkey, the United States and many other places.

23. As Daron Acemoglu and James R. Robinson have noted recently, free societies exist in a "narrow corridor".[21] A free society requires an efficient and powerful state to flourish, or else citizens' freedom will be impaired by forces outside of the state, such as unregulated corporations, criminal gangs or irregular armed groups. Once the state is efficient and powerful, however, it must be checked and controlled by civil society, to ensure that its power is directed at the common good and not at restricting the freedom of citizens. A free society can only exist in the narrow corridor between a weak state that cannot protect its citizens and a powerful, unconstrained state that preys upon them. Whether a country remains within that narrow corridor is uncertain

[19]Larry Diamond, "Facing Up to the Democratic Recession" (2015) 26 *Journal of Democracy* 141 at 141.
[20]Ibid. p. 147.
[21]Daron Acemoglu and James R. Robinson, *The Narrow Corridor: States, Societies and the Fate of Liberty* (Penguin, 2019).

and contingent. Civil society bears significant responsibility for ensuring that it does. Many events can push countries out of the narrow corridor, including in particular the power and risks of technological change. Events in China and India show how the state can harness technology to enhance and concentrate its own power, with damaging consequences for freedom and fundamental rights.

24. We must therefore think carefully about how to manage technological change, both because of its risks and its promise, and particularly because of its potential to redraw the boundaries between citizen and state in favour of the state, and to put at risk citizens' hard-won fundamental rights and freedoms. In the current political climate, these risks are significant. Any society can slip outside the narrow corridor. To avoid that happening, we need be vigilant to ensure that the state remains safely corralled within its boundaries. One of the areas for particular vigilance in the years ahead must be the digital world, where we must work to ensure that its benefits are employed in a manner that do not threaten human rights and democracy.