The global governance of cyberspace: reimagining private actors' accountability: introduction

Eirini Kikarea* and Maayan Menashe**
Editors-in-Chief

1 INTRODUCTION

The advent of the digital revolution brought about a wave of optimism and raised the hopes of societies for better governance and more freedoms, hopes that today seem dashed, at least partly. There is a widespread belief that new and emerging information and communication technologies (ICTs) pose threats to the rights of individuals and groups, and give rise to complex global governance questions. A growing amount of literature shows how they present challenges for data privacy, discrimination, and inequality, economic relationships, human rights and freedoms more generally. With regard to global governance, they have already radically changed the balance of power between public and private actors, they have introduced novel decision-making tools, and have revolutionised communications, turning them into a self-standing challenge.

The diffused pessimism surrounding the design and impact of ICTs on societies is evident from assessments of cyberspace in general and of latest technological developments in particular, especially Artificial Intelligence (AI). For better or worse, the invasion of new technologies in our daily lives is plain to see; we communicate, learn, spend, get entertained, work, and do all sorts of everyday activities using new technologies, in cyberspace. Cyberspace, a word originating from the ancient Greek word 'κυβερνήτης' (governor, steersman), refers to a domain where communication occurs over computer networks.[1] This online environment does not constitute part of a new dimension, as is often assumed, but is linked to hardware facilities located within the territory of states.[2] This realisation is important for understanding which actors are capable of regulating and influencing this sphere and the means available for doing so. Yet despite this territorial link, cyberspace can be seen as a 'global space' because actors from all over the globe contribute and benefit from it simultaneously.[3] Also, new private actors (especially social media companies), whose activities are motivated by profit, are prominent in cyberspace. On the other hand, it appears that AI technologies will quickly and pervasively become part and parcel of modern societies, facilitating important tasks such as medical diagnoses and climate forecasting. Nevertheless, AI in general and machine learning in particular have been subject to widespread criticism. As machines become more intelligent, many questions arise regarding their potential

* University of Cambridge, UK (Onassis Foundation Scholar); email: editors@cilj.co.uk.
** University of Cambridge, UK; email: editors@cilj.co.uk.
[1] Lexico - Oxford University Dictionary, 'Cyberspace' available online <https://www.lexico.com/en/definition/cyberspace> accessed 11 September 2019 ('[t]he notional environment in which communication over computer networks occurs').
[2] Martha Finnemore and Duncan B Hollis, 'Constructing Norms for Global Cybersecurity' (2016) 110 American Journal of International Law 425, 460.
[3] Eyal Benvenisti, 'Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?' (2018) 29(1) European Journal of International Law 9, 79.

harmful impact on human societies. Autonomous weapons, facial recognition and privacy invasion, discrimination, and social media manipulation, are few key concerns raised by AI, already causing headache to policy-makers and adjudicators.[4]

This Special Issue aims to critically assess novel and complex challenges posed by new and emerging technologies, from the perspective of international law. The different papers published in this Issue provide a valuable analysis of a wide range of international law topics related to new and emerging technologies and global governance, underlining challenges and suggesting solutions at both doctrinal and normative level. This important collection of articles combines a rich variety of research methodologies and creates an impactful mosaic of ideas aiming at shaping our understanding and influence future policy-making and dispute settlement in the field of new ICTs and international law.

This introductory article seeks to prepare the ground for this Special Issue, by setting the background and context of the new and emerging technologies, particularly cyberspace, big data, AI, and global governance. It is an attempt to understand recurring themes emerging from the papers' analyses, bring ideas together, and analytically present the combined knowledge exerted from them. The article is divided in two main parts. First, a general overview of key issues currently analysed in literature in the field of new information technologies and global governance, as well as of important challenges that remain largely unaddressed and suggested solutions, is provided. In the second part, the article moves on to identify and further discuss specific themes emerging from the papers included in the Special Issue, and which reflect more generally some of the pressing issues in the field, namely the phenomenon of privatised global governance, power and exclusion in private dominance of cyberspace, new technologies and regulatory gaps, and finally, rights and obligations under international law in relation to cyberspace and new ICTs including the right to access data. Overall, the different approaches, point of views, and indeed, solutions adopted in the various articles, contribute each in its own unique way towards the re-imagining of the notion of accountability for cyberspace, AI, and big data.

2 THE GLOBAL GOVERNANCE OF CYBERSPACE, AI AND BIG DATA: AN OVERVIEW OF CHALLENGES AND POSSIBLE REACTIONS

Technology-related developments shape and influence the daily lives of users, constantly reforming human interactions, political processes, and economic relationships. With greater focus placed on issues pertaining to global governance, this section discusses algorithmic decision-making, access to big data and inequality, new technologies and politics, as well as possible responses to the threats of new and emerging technologies both at domestic and international level.

First, decision-making is rapidly changing with the introduction of algorithms, a theme addressed by a growing amount of literature.[5] Daily, machines take decisions using algorithmic

[4] Matthew U Scherer, 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies' (2016) 29(2) Harvard Journal of Law & Technology 353; Ioannis Kalpouzos, 'Armed Drone' in Jessie Hohmann and Daniel Joyce (eds), *International Law's Objects* (OUP, Oxford 2018); Meredith Whittaker et al, 'AI Now Report 2018' (*AI Now Institute*, December 2018) <https://ainowinstitute.org/AI_Now_2018_Report.pdf> accessed 11 September 2019.

[5] See further Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, Luciano Floridi, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3(2) Big Data and Society 1; Natascha Just and Michael Latzer, 'Governance by Algorithms: Reality Construction by Algorithmic Selection on the Internet' (2016) 39(2) Media, Culture & Society

decision-making. Yet, algorithms are not neutral. They are created by humans and could be designed in a way that replicates biases, beliefs, and stereotypes, which are often unconscious.[6] The results they produce depend on the data they analyse and their learning process, which are highly political.[7] It has also been suggested that algorithms do not produce results on the basis of causation but correlation, understanding issues at population level and not for each individual in question.[8] It follows that the assumptions made by algorithms have the risk of being simplistic and reductionist, and their rigid weighing and balancing of different factors not fit for all scenarios.[9] Moreover, it has been argued that due to their predetermined nature and stereotypical structure, algorithms do not leave room for discretion in decision-making and objectify individuals, undermining human dignity.[10] This discussion is connected with debates on human 'in the loop' and 'on the loop', the first referring to human as a decision-maker that is informed by algorithms and the second to human as a reviewer of decisions produced by the actual decision-maker, the algorithm/machine.[11] Additional negative factors are the expansion of algorithmic decision-making to nearly all areas of human activity, combined with the 'invisibility' of their operation.[12] Platonic metaphors, such as Plato's cave allegory, are employed by scholars to illustrate an emerging 'black box society', a society with increased discriminatory manipulations.[13] All these concerns about unrestrained algorithmic control have led to calls for more accountability in algorithmic decision-making, with recommendations for algorithmic transparency and alternative design methods.[14]

238; Danielle Kehl, Priscilla Guo, and Samuel Kessler, 'Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative' (2017) Harvard Law School Berkman Klein Center for Internet & Society <https://dash.harvard.edu/handle/1/33746041> accessed 11 September 2019; Joshua A Kroll, Solon Barocas, Edward W Felten, Joel R Reidenberg, David G Robinson and Harlan Yu, 'Accountable Algorithms' (2017) 165(3) University of Pennsylvania Law 633.

[6] See for example, Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York, New York University Press 2018); Lauren Goode, 'Facial Recognition Software is Biased Towards White Men, Researcher Finds' (*The Verge*, 11 February 2018) <https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error> accessed on 11 September 2019; Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81(1)-(15) Proceedings of Machine Learning Research 1 <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> accessed 11 September 2019; Bruce Glymour and Jonathan Herington, 'Measuring the Biases that Matter: The Ethical and Casual Foundations for Measures of Fairness in Algorithms' (2019) FAT'19 Proceedings of the Conference on Fairness, Accountability, and Transparency 269. For the claim that algorithms could correct biases see Cass R Sunstein, 'Algorithms, Correcting Biases' (2019) 86(2) Social Research: An International Quarterly 499.

[7] See Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.

[8] Lorna McGregor, 'Accountability for Governance Choices in Artificial Intelligence: Afterword to Eyal Benvenisti's Foreword' (2019) 29(4) European Journal of International Law 1079, 1081.

[9] Benvenisti (n 3) 65ff.

[10] Ibid 65.

[11] McGregor (n 8) 1082.

[12] See further Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge and London, Harvard University Press 2015).

[13] Ibid.

[14] See further Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89(1) Washington Law Review 1; Nicholas Diakopoulos, 'Algorithmic Accountability: Journalistic Investigation of Computational Power Structures, 3(3) Digital Journalism (2015) 398; Mike Ananny and Kate Crawford, 'Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability' (2016) 20 New Media and Society 973; Tal Zarsky, 'The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making' (2016) 41(1) Science, Technology and Human Values 118; Jay Thornton, 'Cost, Accuracy, and Subjective Fairness in Legal Information Technology: A Response to Technological Due Process Critics' (2016) 91(6) New York University Law Review 1821; Chagal-Feferkorn, 'The Reasonable Algorithm' (2018) 2018 University of Illinois Journal of Law, Technology and Policy 111; Kroll et al (n 4) 633; Andrew Tutt, 'An FDA for Algorithms' 69 Administrative Law Review (2017) 83; Pasquale (n 11).

New and emerging technologies have also changed and continue to influence political processes. Foucault has long argued that the way truth is communicated has a great impact on governance.[15] Relying on their ability to drastically change communications, new technologies made a grand promise for a new era of e-democracy, particularly through enhanced transparency, e-decision making, more direct engagement of the public through social media platforms, more opportunities to express one's political views online, and more access to information from the general public.[16] Nevertheless, the relationship between technology and democracy could be proven to be an example that sometimes less is more. More communication does not necessarily lead to more democracy. Today, the abundance and complexity of communication channels have led to an overload of information and news, often contradictory, causing confusion to voters. This is because the attention span of humans is limited and, hence, exposure to numerous political opinions and news, often 'fake', misdirects the focus of users.[17] The solution presented by social media companies to this overload is the process of 'filtering', for instance through the personalisation of newsfeed posts based on the users' preferences.[18] Such practices, however, arguably give rise to more hate speech and deepen political polarisation because users no longer have the chance to get exposed to a diversity of political views.[19] Overall, this information overload combined with the rather obscure operation of algorithms conceals the potential for manipulation of communication channels by both private and public actors and puts democracies at risk.[20]

Another challenge for global governance is big data. Colossal social media companies and some states not only control the channels of communication but also the information provided consensually by their users. Data collected from every corner of the world is assembled together and used for various purposes that could not have been predicted by the data contributors. The withholding and analysis by a few large actors of big data has given rise to the so-called 'big data divide', a modern form of information asymmetry. This divide refers to the fact that the actors having access to big data, are in a position of 'invisible' power compared to those who do not.[21] In a phenomenon, which has been termed as the 'paradox of boundaries', those actors advocate erasing boundaries in order to collect data but at the same time push for the creation of new boundaries to establish exclusive data exploitation rights for themselves.[22] By accessing and

[15] Arnold I Davidson (ed), *Michael Foucault, On the Government of the Living: Lectures at the Collège de France* (Palgrave 2014).
[16] Lincoln Dahlberg and Eugenia Siapera (eds), *Radical Democracy and the Internet: Interrogating Theory and Practice* (New York, Palgrave 2007); Andrew Chadwick, 'Web 2.0: New Challenges for the Study of E-Democracy in an Era of Informational Exuberance' (2008) 5 I/S: A Journal of Law and Policy for the Information Society 9.
[17] Cass R Sunstein, *#Republic: Divided Economy in the Age of Social Media* (New Jersey, Princeton University Press 2017) 17.
[18] Such 'filtering' is used for instance by Facebook, Twitter, and Instagram.
[19] Jonathan Zittrain, 'Facebook Could Decide an Election Without Anyone Ever Finding Out' (*New Republic*, 1 June 2014) <https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering> accessed 11 September 2019; Ryan Calo, 'Digital Market Manipulation' (2014) 82 George Washington Law Review 995; danah boyd, 'Why America is Self-Segregating' (*Points,* 5 January 2017) <https://points.datasociety.net/why-america- is-self-segregatin g-d881a39273ab> accessed 11 September 2019; Sunstein (n 17) 138–139.
[20] See further Edson C Tandoc Jr, Zheng Wei Lim and Richard Ling, 'Defining "Fake News"' (2018) 6(2) Digital Journalism 137; Vian Bakir and Andrew McStay, 'Fake News and the Economy of Emotions' (2018) 6(2) Digital Journalism 154.
[21] Zeynep Tufekci, 'Engineering the Public: Big data, Surveillance and Computational Politics' (2014) 19 First Monday <https://firstmonday.org/ojs/index.php/fm/article/view/4901/4097> accessed 11 September 2019; Krause Hansen and Tony Porter, 'What Do Big Data Do in Global Governance?' (2017) 23(1) Global Governance: A Review of Multilateralism and International Organizations 31; Susan Arial Aaronson, Patrick Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21(2) Journal of International Economic Law 245.
[22] Hansen and Porter (n 21).

analysing big data, these actors possess additional means to achieve their profit-making or other goals, by targeting those that do not have this privilege.[23] This is why it is often said that data is the new oil. Extremely valuable and simultaneously difficult to access by the public, data is the fuel for the development of AI-related products and services, and will possibly be the foundation of modern and future production models.[24] Being linked to automated governance, big data further enhances the role of algorithms and overshadows the human element.[25] In contrast to the arguments of the proponents of big data that the latter will enhance political participation and improve policy-making, there are reasons to believe that big data will lead to opposite results. Given the unintended and passive nature of such participation, the lack of public deliberation, and the presumed neutrality of big data leading to the exclusion of social groups not having access to it, meaningful participation of citizens may in practice be obstructed.[26] Concerns relating to big data have also been voiced in the context of special fields of international law such as human rights.[27]

It becomes apparent that private global players have assumed a central role in the global private governance of cyberspace. The question arises whether domestic and international regulatory initiatives as well as self-regulation through voluntary standards suffice to regulate their activities. Social media companies increasingly engage in rule-making and adjudicative functions concerning fundamental rights, including free speech and privacy, resembling 'privately owned bureaucracies'.[28] In a famous statement by Mark Zuckerberg, it was held that Facebook is more like a government than a private company.[29] This resemblance justifies the adoption of regulatory measures addressed to these private actors, including reasoned decision-making and participation rules, as well as enhanced appeal and transparency measures, such as those recently adopted by Facebook.[30] Nevertheless, up to date self-regulation has proven to be insufficient, despite the existence of several initiatives by large social media companies.[31] The private governance of cyberspace is still largely lacking in legitimacy and accountability, mostly due to the companies' profit-seeking character that has slowed down the adoption of appropriate procedures and norms.[32]

International law lacks a comprehensive approach to technology-related challenges, leaving solutions largely to domestic law. But domestic law is not alone in a position to effectively address these challenges at a global level as it differs largely across national jurisdictions and because it risks becoming overly restrictive for freedoms.[33] However, inspiration can be drawn from the more progressive domestic and regional law approaches adopted during recent years. For example,

---

[23] Mark Andrejevic, 'The Big Data Divide' (2014) 8 International Journal of Communication 1669.
[24] Scherer (n 4) 354.
[25] Hansen and Porter (n 21).
[26] Michal Saliternik, 'Big Data and the Right to Political Participation' (2019) 21 University of Pennsylvania Journal of Constitutional Law 713.
[27] Helmut Philipp Aust, "'The System Only Dreams in Total Darkness': The Future of Human Rights Law in the Light of Algorithmic Authority' (2017) 60 German Yearbook of International Law 71. See also on data and international law, Steven Humphreys, 'Data: The Given' in Hohmann Joyce (n 4) 191.
[28] Hannah Bloch-Wehba, 'Global Platform Governance: Private Power in the Shadow of the State' (2019) 72 SMU Law Review 27.
[29] See Ezra Klein, 'Mark Zuckerberg on Facebook's Hardest Year, and What Comes Next' (*Vox*, 2 April 2018) <www.vox. com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge> accessed 11 September 2019.
[30] Lorenzo Casini, 'Googling Democracy? New Technologies and the Law of Global Governance: Afterword to Eyal Benvenisti's Foreword' (2019) 29(4) European Journal of International Law 1071, 1075.
[31] Benvenisti (n 3).
[32] Ibid 72-5.
[33] Ibid 65-6.

several states have already proceeded to the recognition of the right to privacy and the more specific right to personal self-determination' and the right to be forgotten, protecting individuals against the unrestricted collection and use of their personal data.[34] Worth mentioning is also the General Data Protection Regulation (GDPR) adopted by the European Parliament, including among others minimal rules on automated decision-making.[35]

The limitations of domestic law show that there is a role for international law to play. Scholars have adopted the view that existing pre-cyber international law norms apply to novel cyber-related activities.[36] Commentators have also suggested the creation of a single international cyberspace framework, focusing on issues such as intellectual property theft, restrictions to the free flow of data, cyber security concerns, and privacy.[37] Other solutions that have been put forward are the creation of a global Internet body[38] or creating special forms of control over large social media companies that operate as de facto monopolies.[39] However, the conclusion of a treaty with a truly global reach that would include overarching solutions on issues related to new technologies is rather unrealistic and appears to be unattainable for now. This is due to the disparate approaches of states on core concepts and approaches that would lead to great disagreements jeopardising the whole endeavour.[40]

In an attempt to surpass the limitations of domestic law, Eyal Benvenisti envisages cyberspace in general and big data specifically as global commons, arguing regarding an aggregate and anonymised version of big data as a shared-access resource in international law.[41] By making an analogy with watercourses law, Benvenisti submits that the freedom to have access to data is necessary for accountability purposes.[42] What matters according to the argument is not the ownership of data, which may be public or private, but its status and the rights and obligations connected therewith, particularly the duties towards users and states. This global commons argument serves as a useful lens through which to consider some of the common themes that can be identified throughout this Special Issue.

Following Benvenisti's reasoning, big data exists on the basis of contributions made by millions of users from all over the world on a daily basis.[43] They are large pools of information contributed by domestic and foreign users that, on aggregate, constitute valuable sources of knowledge that could be used to the benefit of mankind. To legally conceptualise big data,

---

[34] See for instance Steven C Bennett, 'The Right to Be Forgotten: Reconciling EU and US Perspectives' (2012) 30 Berkeley Journal of International Law 161.

[35] See article 22 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR); See Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2017) 38(3) AI Magazine 50.

[36] See for instance Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge, CUP 2017).

[37] Richard N Hass, 'World Order 2.0: The Case for Sovereign Obligation' (2017) 96 Foreign Affairs 2.

[38] See further Martha Finnemore and Duncan B. Hollis, 'Constructing Norms for Global Cybersecurity' (2016) 110(3) American Journal of International Law 425; Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers' (2017) 30 Leiden Journal of International Law 877.

[39] Casini (n 30) 1077; Franklin Foer, *World without Mind: The Existential Threat of Big Tech* (Penguin 2017).

[40] For example, see the lack of consensus of in the context of the Group of Governmental Experts on advancing responsible state behaviour in cyberspace for international security (GGE). See further, Anders Henriksen, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace' (2019) 5(1) Journal of Cybersecurity 1.

[41] Benvenisti (n 3).

[42] Ibid 61.

[43] Ibid 80-1.

Benvenisti invokes the concept 'common heritage of mankind'.[44] This concept emerged to address concerns in connection with global commons, namely global, international, supranational spaces of common resources, usually beyond national jurisdictions. 'Commonality' mainly refers to the idea that collective benefits will accrue from the protection of a resource or from tackling common concerns,[45] and 'heritage' to the need for sound management of a resource to be passed to heritors.[46] Common concerns may be global in character, such as climate change, or could relate to resources found within national boundaries, such as biodiversity. The term 'common heritage of mankind' legally entails that no one should be restricted from accessing certain resources that belong to everyone, including future generations and developing states.[47] It is a normative concept that demands not only open access but also public regulation of resources that would distribute costs and benefits by creating rights for the public and imposing responsibilities to the holders of the resources. Common heritage protects common areas and resources outside national jurisdictions from international claims, and imposes responsibility for the protection of the common good for the benefit of all mankind when it is located within national borders. According to Benvenisti, only if governments, monitoring agencies, and other governance bodies gain access to big data owned by private and public entities and used in the context of algorithmic decision-making, will it be possible to tackle modern and future technology challenges. This conceptualisation of big data and cyberspace as global commons enables policy-makers to imagine and design a more equitable international framework capable of addressing complex contemporary challenges.

Moreover, despite difficulties in reaching consensus globally, the international community is arguably in a position to agree on focused solutions tackling specific governance issues related to new technologies, even minimally. For example, with regard to elections, a viable solution, already implemented by several states, would be to establish reliable neutral bodies/websites that would review the content of news to check their objectivity and identify 'fake news'.[48] At least at first level, an approach similar to the one followed in the context of international environmental law negotiations could be adopted, namely establishing initially a general framework of principles regulating the specific issue in question and then further develop the framework by adopting more specific obligations usually in the form of Protocols.[49] This technique would enable policy-makers

[44] On the history of this concept see Surabhi Ranganathan, 'Global Commons' (2016) 27(3) European Journal of International Law 693; See further Isabel Feichtner and Surabhi Ranganathan, 'International Law and Economic Exploitation in the Global Commons: Introduction' (2019) 30(2) European Journal of International Law 541; Matt Craven, 'Other Spaces': Constructing the Legal Architecture of a Cold War Commons and the Scientific-Technical Imaginary of Outer Space' (2019) 30(2) European Journal of International Law 547.

[45] Jutta Brunnée, 'Common Areas, Common Heritage, and Common Concern' in Daniel Bodansky, Jutta Brunnée, Ellen Hey (eds), *The Oxford Handbook of International Environmental Law* (OUP 2018).

[46] Tullio Scovazzi, 'The Concept of Common Heritage of Mankind and the Genetic Resources of the Seabed beyond the Limits of National Jurisdiction' (2007) 25 Agenda Internacional Año XIV 11, 12 footnote 4.

[47] Ranganathan (n 42) 694.

[48] Casini (n 30) 1077.

[49] See for example, Vienna Convention for the Protection of the Ozone Layer (adopted 22 March 1985, entered into force 22 September 1988) 1513 UNTS 293, and the Montreal Protocol on Substances that Deplete the Ozone Layer (adopted 16 September 2987, entered into force 1 January 1989) 1522 UNTS 3; United Nations Framework Convention on Climate Change (adopted 9 May 1992, entered into force 21 March 1994) 1771 UNTS 107 and Kyoto Protocol to the United Nations Framework Convention on Climate Change (adopted 11 December 1977, entered into force 16 February 2005) 2303 UNTS 162; Convention on Biological Diversity (adopted 5 June 1992, entered into force 29 December 1993) 1760 UNTS 79 (CBD) and its two protocols, i.e. the Cartagena Protocol on Biosafety to the Convention on Biological Diversity (adopted 29 January 2000, entered into force 11 September 2003) 2226 UNTS 208 and Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization to the Convention on Biological Diversity (adopted 29 October 2010, entered into force 12 October 2014) 30619 UNTS 3009.

to adapt the special regimes in parallel to an evolving understanding of the role of technology in modern societies, without risking leaving present and pressing concerns completely unaddressed. Regulatory initiatives of this kind should arguably attempt to take into account competing interests of affected communities and businesses, and be envisaged in alignment with the principles incorporated in existing international frameworks.

In addition to the development of such special frameworks, it is also pivotal to proactively scrutinise ICTs' wider influence on governance choices.[50] Governing bodies are often presented with the option to use technological tools that would facilitate the implementation of their tasks or mandates. Yet, this will greatly change the way these bodies operate and carry out their functions, presenting significant governance risks.[51] These risks are further heightened by the fact that the users of new technologies neither participate in their development nor in the decision to incorporate them in governance, despite the fact that it is the users that are potentially negatively impacted by them. To avoid the adoption of costly and possibly inefficient adaptation measures, it is preferable to proactively assess how information technologies might impact specific governance choices and structures rather than to merely respond to challenges created by the new forms of governance at a later stage. This approach will also enable re-establishing trust and confidence in public bodies.[52] In the long run, legal responses will not suffice to address these challenges unless states focus on educating their citizens on new and emerging technologies and their role in modern societies, so that they can better understand their inherent limitations.[53]

All the above allow the conclusion that the complicated and uncertain nature of the challenges presented by new ICTs necessitate a multidimensional approach both at global and domestic level, and enhanced cooperation between public and private actors, and epistemic communities. In this Special Issue, an attempt is made to outline the benefits of an interdisciplinary legal glance to contemporary threats by new technologies, recognising at the same time the need for further research investigating these concerns.

3 EXPLORING CRITICAL EMERGING THEMES THROUGH THE LENS OF THIS SPECIAL ISSUE

This section will further build upon Benvenisti's characterisation of cyberspace as an accessible global commons, by exploring critical themes emerging from this perspective and showing how they come into play in the discussions presented in this Special Issue. These themes include both the features rendering the global commons characterisation as suitable to cyber communications and big data as well as the implications resulting from such a characterisation. The different articles published in this Issue provide a valuable concretisation of these ideas through a wide range of topics. The first theme that is identified is the current privatised nature of global governance, as a result of the prevalence of new ICT technologies. The second highlighted theme focuses on some of the concerns arising out of such privatised cyberspace, and in particular the exclusion of vulnerable groups and the influence of private, profit-driven actors. The third theme deals with the

[50] Lorna McGregor (n 8) 1083.
[51] Ibid 1084.
[52] Ibid 1083.
[53] Casini (n 30) 1077.

current regulatory gap when it comes to new ICTs and cyberspace, which exacerbates the problems of the current states of affairs. Finally, some of the solutions offered in this Special Issue will be presented, focusing on the role of international law as well as the need to assure a wider access to big data. Taken together, this important collection of research demonstrates the relevance of these recurring themes to current pertinent issues of new and emerging technologies and international law.

3.1 Privatised global governance

As discussed, the private actors that gather, control, and utilise mass databases hold a significant influence over our lives. The predominance of big data in so many aspects of modern society means that these private actors have de facto the power to shape the world we live in, and often engage in governance functions traditionally performed by public actors. This form of private governance opens the door for ICT companies to exercise power over peoples' individual freedoms and possibly infringe upon their human rights. Their influence often extends beyond users that sign up to their services consensually, affecting non-related third parties in various ways.

Benedict Kingsbury, in his article that opens this Special Issue, puts forward the idea of 'infrastructure as regulation' as means of thinking about international law, technology, and society. As part of this idea, Kingsbury argues that infrastructure, including digital infrastructure, 'can (and often does) operate in some significant relation to law. In crude simplification, infrastructure may be a means of implementing law, or of enabling law. It may be a substitute for law, or displace law. It may be an obstacle to law or prevent law, or interact pathologically with law. Infrastructure may create dependencies, engender cooperation, or structure conflict.' Kingsbury explains in this respect that, just as with major physical infrastructures, the infrastructural choices made by digital platform companies can have real effects on social order, including on human and civil rights and de facto limit regulatory possibilities. By making such choices, these companies are therefore exercising what he refers to as 'opportunity-structuring powers'.

The overarching impact of private actors is evident in a variety of areas, as reflected in the papers published in this Special Issue. The article by Mark Leiser relates to the central role of social media platforms as part of a contemporary public sphere, contributing to a 'marketplace of ideas'. In this context, the author examines how these platforms are used for the dissemination of disinformation within a 'computational propaganda'. The article acutely demonstrates the potential harmful influence of activities within private platforms on society as a whole. The negative effects identified by the author are as broad as their contribution to public health crises, rise in climate change scepticism, the manipulation of voters, and the interference with democratic deliberation.

Petra Molnar's article directly shows how new technologies and big data operated by private actors participate in public regulatory functions, while affecting a vast number of migrant populations. In her article, the author discusses the usage by states and international organisations of different technological experimentations driven by private sector innovation as part of 'migration management' activities. According to the author, the way these new technologies are currently used result in human rights infringements, by leading *inter alia* to discrimination, privacy breaches, and procedural fairness issues, with far reaching ramifications for immigration and refugee implementations.

Yseult Marique and Enguerrand Marique also deal with the public-private 'hybridity' of new ICT companies, specifically platform providers, by focusing on their role in imposing sanctions. The authors describe how platform providers are delegated with powers by public authorities to monitor and enforce particular norms online. However, as the authors describe, when doing so, these private entities hold discretion with regards to gaps that need to be filled in these norms. As such, they perform roles that are similar to sovereign bodies in terms of norm-setting and the application of sanctions. According to the authors, platform providers' actions therefore deeply affect the individual freedoms of users.

Similarly, Paolo Cavaliere's paper relates to platforms' 'power to govern the flow of information at the global level', and in particular to their role as regulators of content, while focusing on online acceptable speech. As in the paper of Marique and Marique, Cavaliere discusses in his article how private companies were also guided by public authorities to take on these roles, through the passing of the EU Code of Conduct on hate speech. The author examines the relevant terms of service of the platforms, arguing that they hold a substantial normative role to the point that they complement or even supersede pre-existing legal standards. He concludes that the platforms' policies expand the scope of speech that can be restricted, with resulting concerns for the impact on individuals' freedom of expression.

Finally, Rachel Adams and Nóra Ní Loideáin also touch upon the influence of private ICT companies on the global sphere. This paper describes how virtual personal assistants reproduce negative gender stereotypes and as such perpetuate indirect discrimination against women. As the authors explain, the problems they recognise do not only affect the users who chose to use products such as Apple's Siri and Amazon's Alexa, but also have broader implications, as these AI technologies are increasingly present in environments such as in banks, cars, and workplaces.

3.2 Power and exclusion in private dominance of cyberspace

The described dominance of private ICT companies in the global online sphere raises a set of concerns, creating 'winners' and 'losers' in contemporary cyberspace. First, as discussed, the growing reliance on big data can be problematic when the source of this information is the private marketplace.[54] That is, this data is gathered, controlled and used by private companies that are motivated by profit maximisation, raising concerns over its accuracy and reliability. This information can be manipulated by these private actors to gain more profits and political power.[55] In addition, big data is susceptible to false information, misrepresentations, and biases. The role of information in the era of new ICTs has deepened power asymmetries while creating new ones: both between the ICT corporations and the affected users, and also between different segments of users, empowering those who have better access to this data.[56]

These concerns are reflected in the article of Louise Arimatsu in this Special Issue. Arimatsu explores the role of new digital technologies in reproducing and amplifying the patriarchal structures, practices, and culture of contemporary life. She argues that, in doing so, new and emerging technologies operate to silence women through exclusion and online gender-based

[54] Hansen and Porter (n 21); Tufekci (n 21).
[55] Pasquale (n 12).
[56] Benvenisti (n 3) 60–61, 67–71.

violence. Among the problems the author describes is the exclusion of women from access and use of new ICTs which only deepens the existing gendered power differentials. Moreover, Arimatsu explains that with the growing role of new technologies, it is even more problematic that women are deprived from the opportunities to influence the trajectory and content of this technology.

The exclusion of women from new ICTs and the problems associated with this phenomenon are also discussed by Adams and Ní Loideáin in this Issue. The authors describe how the gender stereotypes that are reflected in virtual personal assistants 'ha[ve] material consequences for women and the expectations of women in society'. Reinforcing the concern addressed by Arimatsu regarding the exclusion of women from ICTs, the authors explain that stereotyping women negatively in the context of virtual personal assistants products may well be the result of the gender inequalities and poor representation of women in the tech sector, which is responsible for the design of these technologies.

Migrants constitute another marginalised population bearing the burden of new technologies at the hand of private actors. In her article, Molnar submits that what makes it acceptable for countries to carry out technological experiments on migrants is exactly their status as non-citizens, and their consequent exclusion from social and political life. This is particularly true when considering the vulnerability of migrants, as well as the North-South power asymmetries inherent in the proliferation of new and emerging technologies. In that sense, the author explains, by not taking into consideration the experiences of migrants and with lack of oversight and accountability, new technologies only replicate existing power hierarchies and differentials.

The concern that big data intensifies different power asymmetries is also echoed in the article by Marique and Marique. The authors describe the market power of platform providers compared to the power of users, in terms of their data and revenues, while also relating to the fact that platform providers benefit from the lack of real market competition. In these circumstances, the authors discuss how platform operators are able to 'organise individuals' lives and impose upon them terms which are neither negotiated nor to which individuals are party'. Among other considerations, these observations lead the authors to question the legitimacy of such private rule-making processes.

Finally, the article by Shannon Raj Singh demonstrates the negative consequences arising when profit-driven companies govern ICTs from a different angle. Focusing on the realm of international criminal law, the author explores the role of social media entities in fuelling atrocity crimes through the lens of complicity. In this context, the author describes how social media platforms operate to gain profits by increasing the user engagement with the platform. One of the results of this motivation is the development of algorithms that 'target primal negative human emotions', which serves to drive extremism, leading the author to explore the analogy of social media as a weapon.

3.3 New ICTs and the regulatory gap

Borrowing Kingsbury's words in this Special Issue, the international legal framework for ICTs' challenges 'is at present scanty, woefully lagging, and in urgent need of construction.' Following the global commons argument, another feature of new ICTs is that in the absence of an international approach, these activities run the risk of remaining insufficiently regulated. As Benvenisti estimates, '[t]he prevailing assumption seems to be that matters of ownership of, and access to, cyber communications and data are subject only to domestic regulation and that international law is silent

on such issues'.[57] Yet, as discussed above, similarly to other issues in the contemporary globalised world, the transnational reach of these actors and activities can lay obstacles on national regulations by itself simply ineffective. An additional layer of complication is present due to the private ownership of mass databases. The contractual relationships that organise the different interactions between actors can serve as an argument against the interference of domestic public laws. Moreover, public bodies sometimes delegate functions to private actors precisely to avoid being confined to certain regulations.[58] In these circumstances, ICT companies are left to design their own regulation. Such self-regulation, again, invokes a series of concerns, of the kind that arise in situations where private actors regulate their own conduct.

The article by Arimatsu in this Special Issue reflects this regulatory gap, arguing that states fail to meet their international human rights obligations on discrimination against women, focusing in particular on the 1979 Convention on the Elimination of All Forms of Discrimination against Women.[59] In addition, as the author explains, there are currently no direct human rights obligations for companies under international law. The result is 'the silencing of international law', which 'is made possible by the constitution of the digital space as a privatised public space'.

Relatedly, Adams and Ní Loideáin explore provisions and findings within international women's rights law to elucidate the fostering of gender stereotypes in virtual personal assistants. Among the applicable legal instruments, the authors show the relevance of the United Nations Guiding Principles on Business and Human Rights (UN Guiding Principles) in providing guidance to states and private actors on their human rights responsibilities. However, in light of the non-binding nature of these provisions, the authors underscore gaps in implementation and enforcement. They conclude in this respect that 'the critical concern for international human rights law is how to hold the private sector to account for the reproduction of negative gender stereotypes and the social harm this causes in terms of indirect discrimination against women'.

As aforementioned, Marique and Marique describe the sanctioning power that platform providers currently hold. However, as they explain, despite these regulatory functions, platform operators enjoy discretionary power, 'discretion which is very little constrained by either procedures or substantive principles, as self-regulation mainly applies'. Similarly, Leiser also relates to the self-regulating power of online platform providers. While in some cases, such as in the instances explored in the paper of Arimatsu and that of Adams and Ní Loideáin, states are under international obligations to regulate the activities of private actors, even if these obligations are not met, Leiser assesses that there is 'no coherent legal framework to hold states responsible' for computational propaganda. The regulatory gap here is thus twofold; private actors are not sufficiently regulated and states do not have an obligation to regulate these activities.

Molnar also shows that migration management is another issue that suffers from the lack of governance of new and emerging technologies; there are currently no clear enforceability mechanisms binding states engaged in these activities. Moreover, these activities are often carried out by international organisations, which are subject to even fewer legal obligations and accountability mechanisms. As the author puts it, 'technological experimentation in migration occurs in opaque spaces where state accountability is weak'. The article boldly argues that such

[57] Benvenisti (n 3) 79.
[58] Ibid 41.
[59] Convention on the Elimination of All Forms of Discrimination Against Women (adopted 18 December 1979, entered into force 3 September 1981) 1249 UNTS 13.

regulatory gap is deliberate on states' part. According to the argument, states outsource responsibility for technological innovation to the private sector precisely in order to be discharged from human rights restrains while testing new technologies, creating a differentiation of rights between citizens and non-citizens.

3.4 Rights and obligations under international law and the right to access data

The argument that cyberspace should be treated as global commons underscores the need for meaningful regulation at the international level. It has been repeatedly emphasised that the transnational nature of cyberspace can render national regulation, by itself, insufficient. National laws can regulate certain aspects of the gathering and usage of data within its territories. However, there will be issues remaining outside the scope of application of domestic law or outside its scope of interest. The papers in this Special Issue show, through a range of topics, the wide overreach of new ICTs: affecting citizens, users, women and migrants, to name a few. As big data influences the lives of people from around the globe, the regulatory response should arguably take these individuals into consideration. In such circumstances, more robust international rights and obligations will reflect this need for international oversight over the operation of new ICTs. To this end, the articles in this Special Issue provide additional force and grounding to the call for regulation of cyberspace in international law. They examine, each adopting a very unique viewpoint, how international law can address the regulatory gaps described and ensure more accountability and transparency in the operation of private ICT companies. A recurring theme among the different articles is the call for more access to information, in a way that would give voice to all those negatively affected.

The first article by Kingsbury responds to the need to adapt international law to technological changes by 'thinking infrastructurally'. As aforementioned, this entails the recognition that infrastructural choices operate as regulation. Following this line of thought, the paper explores the implications for reinvigorating deliberative forward-planning international law projects to address technologically-driven transformation. The article identifies several desirable legal shifts in this regard, including the collective representation and governance of infrastructures, more far-sighted and participatory planning, mapping out the routes of different paths before they are chosen, financial and data planning, and bringing into the discussion holistic values and justice considerations.

In her paper, Arimatsu considers how international human rights law can be harnessed to counter the silencing of women through the developments in new digital technologies. The 'constitution of the digital space as a privatised public space' leads the author to consider not only states' human right responsibilities, but to also explore the possibility of establishing direct human rights obligations for companies under international law. As part of the steps that should be taken, the author highlights the importance of women's access to new technologies – validating the idea that data should constitute as shared access resource. According to her argument, also put forward by Adams and Ní Loideáin, access to and participation of women in the development of new technologies is important for ensuring equality in their use and design. As Arimatsu concludes, 'only when women are at least equal participants and partners in this field that we might begin to

see a greater diversity and plurality of views not only in the design, development, and content but also in the purpose of digital technologies'.

Adams and Ní Loideáin similarly explore states' obligations under international human rights law to protect women from direct and indirect discrimination 'at the hands of private actors'; and, they too relate to the responsibility of private companies to respect human rights. The authors review relevant instruments of the 'international women's rights canon', including, as aforementioned, the UN Guiding Principles. The authors attribute the lack of compliance with the UN Guiding Principles to the absence of an adequate and effective implementation and enforcement regime. Accordingly, they draw lessons from the EU GDPR and suggest addressing this gap through local governance structures at domestic level that could provide regulatory and oversight functions.

Another suggestion on mechanisms to hold actors involved in ICTs accountable can be found in Leiser's paper. As a response to what the author identifies as lack of regulatory oversight over actors' responsibility for the flow of computational propaganda, the article suggests, among other things, to increase accountability of digital political advertising by providing more transparency with regards to political advertisers. This suggestion supplements Benvenisti's argument of cyberspace as a shared access resource, as it would allow users 'to access information about who has targeted them [with political advertisement] and by what means'. This suggestion empowers users with more information on the online activities they are exposed to as well as ensures more informed democratic decisions on their behalf.

Molnar's paper relates to the need to ensure more access to big data, while discussing some of the human rights concerns resulting from the technological experimentation in migration management. The author describes the practice of collecting vast amounts of data, including biometric identification from migrants. Given the vulnerable position of migrants, it is questioned whether there is real consent on their behalf, which only accentuates the privacy concerns from these practices. As the author explains, with the lack of a sufficient sharing accountability mechanism, there are concerns that the agencies collecting this highly private data would share it with other countries and agencies and even with the private sector. At the same time, as the author explains, there are questions whether the migrants themselves will be granted access to this data. This is a vivid example of the aforementioned big data divide presented above, illustrating the importance of providing shared access to data, especially to those affected by it, in a way that would contribute to the accountability of these processes and mitigate against the great power asymmetry existing in these situations.

In her article, Raj Singh discusses the need to hold, in certain cases, private ICT companies accountable under international criminal law, focusing, as mentioned above, on social media entities and their role in spreading hate speech and fuelling atrocity crimes. The application of international criminal law, according to the author, may be particularly effective in altering the behaviour of these companies, as the criminal prosecution is likely to be calculated into their cost-benefit analysis. Moreover, the author argues, this form of accountability may be more effective in altering the companies' behaviour than non-legal solutions, which tend to be both highly politicised and ineffective. In certain cases, prior to the accountability route under international criminal law, Raj Singh suggests applying in first instance a unique 'independent alert mechanism' which could be used for reporting these illegitimate uses of social media, allowing them to quickly change their behaviour. The suggested mechanism centres on the involvement of local communities affected by

the actions of the social media companies. It reflects the understanding that big data is truly global and cannot be regulated without taking due regard to the different cultures and communities it affects. This 'alert mechanism' thus serves as another illustration of how cyberspace can be regulated in a way that will give more voice and access to the people it affects.

This need to ensure that new ICTs do not operate in a way that disregards local communities and populations is also highlighted in Cavaliere's paper. As aforementioned, the author shows how platform providers regulate and create norms on online speech. The problem, as the author shows, is that while there is no common approach to this matter across different countries, the uniform norms that the platforms impose are likely to 'erode spaces to cater for local, historical, cultural specificities and reduce levers for states to control the boundaries of acceptable speech'. This concern, as in the other described cases, pushes towards regulatory models of new ICTs taking into consideration their nature as global commons by giving meaningful voice to the affected local communities.

Finally, the article by Marique and Marique also proposes a form of accountability on new ICT companies through the involvement and empowerment of the affected stakeholders. As a response to the need of regulating sanctions imposed in digital platforms, the authors suggest including different stakeholders and professionals in this process, while making sure all relevant actors are involved, including the less powerful ones. Together, they will take part in the definition and enforcement of the rules. This, according to the authors, will 'form the backbones of epistemic communities and expertise in online rule-making and sanctions'.

4 CONCLUSION

We have seen that alongside the hopes and benefits associated with the rise of new and emerging ICTs, this phenomenon also introduces a set of acute concerns. As this Special Issue demonstrates, challenges to contemporary global governance span through a wide range of topics and are constantly uncovering. And, indeed, the stakes are high, as ICTs already influence our lives immensely. This introductory article has therefore stressed the need to address the current regulatory gap related to cyberspace, big data and AI, focusing in particular on private actors' accountability. The set of responses and solutions offered by the different authors in this Special Issue will hopefully invite further research on this important topic towards a more robust global governance of ICTs.

Acknowledgments

This Special Issue, Volume 8(2) of the Cambridge International Law Journal (CILJ), gathers a selection of the finest papers presented at the 2019 Cambridge International Law Conference (held on 20th and 21st March 2019). We would like to firstly express our sincere gratitude to the work and efforts of the Conference Convenors, Neli Frost and Rolando Seijas, who together with the Conference Team did an incredible job in continuing our annual tradition here in Cambridge, and hosted once again a stimulating and rich conference, truly reflecting some of the current cutting-

edge research on the topic of ‘New Technologies: New Challenges for Democracy and International Law’.

We are also extremely grateful for the work of the Journal’s Managing Editors, Tim Clark, Catherine Drummond, Patrick Simon Perillo, Francisco Quintana and Faidon Varesis, as well as the work of the General Editors, who’s excellent editorial work enabled this Special Issue to come into life. Catherine Drummond and Patrick Simon Perillo will take over as the forthcoming Editors-in-Chief, and we are confident that the Journal will continue to thrive in their hands.

We would also like to thank the Honorary Editor-in-Chief of the Journal, Professor Eyal Benvenisti, for his remarks in opening the Conference and his presentation on ‘“An AI for an AI”: Toward Algorithmic Checks and Balances’, as well as the members of the Academic Review Board, for their invaluable contribution at the review stage for this Special Issue. Thanks also go to the Journal’s Treasurer Ivan Lee as well as the Blog Manager Beril Boz and the team of Blog Editors, for their continuous support and diligence throughout the year. Finally, we are thankful for the excellent work of the team at Edward Elgar Publishing, including Ben Booth, Marina Bowgen, Katie Smith, and Nick Wilson.