ELTE LAW JOURNAL

ELTE LJ | 2024/2

ELTE
LAW

ELTE LAW JOURNAL

2024/2
ELTE LJ

ELTE
EÖTVÖS
UNIVERSITY
PRESS

Budapest, 2024

ELTE Law Journal is a peer-reviewed periodical published twice a year under the auspices of the ELTE Faculty of Law since 2013.
The publication of this issue was supported by the ELTE Journal Development Fund (ELTE Folyóirat-fejlesztési Alap).

Contact • eltelawjournal@ajk.elte.hu
Eötvös Loránd University, Faculty of Law • 1053 Budapest, Egyetem tér 1–3, Hungary
For submission check out our submission guide at ojs.elte.hu/eltelj

Recommended abbreviation for citations: ELTE LJ

DOI: 10.54148/ELTELJ.2024.2

ISSN 2064 4965

Editorial work • ELTE Eötvös University Press
H-1088 Budapest, Múzeum krt. 4.

ELTE | EÖTVÖS UNIVERSITY PRESS

ELTE EÖTVÖS LORÁND UNIVERSITY

eltebook.hu

Executive Publisher: the Executive Director of ELTE Eötvös University Press
Layout: Andrea Balázs
Printed by: Multiszolg Ltd

Contents

Articles

Jeremy Webber*

Towards a Truly Democratic Constitutionalism**

Abstract

As constitutional scholars, we can fall into the error of treating constitutionalism as though it were primarily about limiting government. This article emphasises that the primary aim of constitutionalism ought to be to *enable* democratic governance, not constrain it. It treats democratic self-determination as having two components: 1) a commitment to building mechanisms by which the people are enabled to participate materially in their own governance on a basis of rough equality; and 2) a commitment to ensuring that the people see themselves as being governed by processes that they consider legitimate. Democratic self-government can take different forms in different societies, but there must be effective mechanisms for citizens – actual citizens, not notional citizens – to govern themselves collectively. The paper sketches some characteristics of a constitutionalism that meets those requirements. It also affirms that, for the people to govern themselves, a constitution must, in a real sense, take the people as it finds them, not impose a partial and caricatured definition upon them. This paper is a prolegomenon to such a constitutionalism, not a description of its totality. The latter is, of course, the work of we as citizens, and as constitutional scholars, through time.

Keywords: constitutionalism, democracy, democratic governance, populism, the people

* Doctor et professor iuris constitutionalis honoris causa, Eötvös Loránd University, Professor Emeritus, Faculty of Law, University of Victoria.

** This is a modestly revised text of Professor Webber's lecture presented to the ELTE Faculty of Law on 9 May 2024.

I Introduction

I begin by expressing my gratitude, my delight, at the honour that this university – Eötvös Loránd University – will be conferring on me tomorrow. It is a very great honour, one I will treasure.

And I am especially pleased that tomorrow I will become (in a sense) your colleague as 'Doctor et professor honoris causa'. I greatly admire the work of your faculty, especially those members with whom I am especially familiar: your public lawyers. It was the leadership of Eszter Bodnár, Zoltán Pozsár-Szentmiklósy and other members of your faculty in developing a new network of constitutional lawyers – the Central and Eastern European regional cluster of the International Society for Public Law – that formed the foundation of my connection to ELTE in the first place.

In fact, I have the distinct sense that I should be honouring you, not the reverse. I have learned so much from my engagement with Hungary over the years. The early part of my academic career coincided with your great constitutional transformation in 1989. I first came to Hungary in 1995 for a series of seminars organised by the Hungarian Academy of Sciences and the Royal Society of Canada.[1] I was then an Associate Professor on the Faculty of Law of McGill University and, after the seminar, we at McGill recruited a young legal and political theorist from the Hungarian Academy of Sciences (Péter Béndek) to occupy the Boulton Fellowship at McGill for a year.

The transition from communism in Hungary posed important questions to all of us interested in legal theory and constitutional law: How does one re-establish the rule of law in a country from which it was lacking for so long? How does one create a viable democratic order? How does one manage the tensions that exist in any democratic order, including tensions over who constitutes the very people in whose name a democratic state is governed? Those are perennial questions in all democratic nations. They are profoundly important, at the heart of our discipline. It was therefore a great privilege, a great opportunity, to learn from your efforts to answer them – practically, effectively and insightfully – in Hungarian society.[2]

And of course those questions have not gone away, not in Hungary, not in any society. Imagine my delight in 2017, just as my term as Dean at the University of Victoria was

---

1 The papers from those seminars were published in Kálmán Kulcsár and Denis Szabó (eds), *Dual Images: Multiculturalism on Two Sides of the Atlantic* (Royal Society of Canada and Hungarian Academy of Sciences 1996, Budapest). My contribution was 'The Rule of Law Reconceived' at pages 197–207.

2 In 2000, I participated in a second project that engaged with the post-communist legal transition in Hungary, although that project addressed Central and Eastern Europe as a whole and its symposium was held at the European University Institute. See Webber, 'Institutional Dialogue between Courts and Legislatures in the Definition of Fundamental Rights: Lessons from Canada (and elsewhere)' in Wojciech Sadurski (ed), *Constitutional Justice, East and West: Democratic Legitimacy and Constitutional Courts in Post-Communist Europe in a Comparative Perspective* (Kluwer Law International 2002, The Hague) 61–99.

approaching its end, to be invited to re-engage in such conversations with you[3] – indeed with a network of dedicated scholars from across Central and Eastern Europe – a re-engagement which has led to many things: to the continuing relationship between your Faculty and ours at the University of Victoria, to the courses and lectures that Eszter Bodnár, Réka Somssich, Zoltán Pozsár-Szentmiklósy, János Mécs, Sára Hungler, Bernadette Somody and Krisztina Rozsnyai have delivered at the University of Victoria, to a graduate course on Democratic Constitutionalism that I taught here at ELTE with Eszter in 2019, and to a major international conference on 'Constitutionalism in a Populist Age', which our two faculties organised at Victoria in March 2020 just as international exchange was shutting down as a result of COVID-19. It seemed as though that conference was the last international conference in the world. Indeed, three of your scholars – Dean Pál Sonnevend, former Dean Attila Menyhárd and Professor Fruzsina Gárdos-Orosz – were unable, at the last minute, to travel to the conference because of the start of the pandemic. That conference has now given rise to three special issues in international journals.[4]

So I have gained much from our many conversations. To be clear, I do not presume to be an expert on Hungary. In relation to Hungary I am merely a student, not a teacher. But those conversations continue to inform my work in legal theory and comparative constitutional law. Today I want to return to the theme of that jointly-sponsored conference of ours: 'Constitutionalism in a Populist Age'. That topic will allow me both to extend our conversation on such questions and to situate that discussion against the backdrop of the career for which you are honouring me (hence the predominance of my work within the footnotes).

Often, the challenge of populism is addressed by constitutional lawyers as a question of limits: Are populist governments complying with the constitutional constraints that apply to them? From that point of view, the problem of populism seems to be one of failing to respect the due constraints on government, failing to stay within the boundaries of democratic action, perhaps even too much democracy. Treating the challenge of populism as being essentially about limits is, I think, a mistake. It acquiesces in seeing constitutionalism as essentially anti-democratic – as a constriction, potentially a frustration, of democratic governance, when in fact constitutionalism developed in lockstep with democracy and continues to be interdependent with it. As a result, the moral high ground of democracy is surrendered to the populists at a time when populist parties – and I should make clear that

---

[3] The occasion was an International Symposium on 'What Can Central and Eastern Europe Learn from the Development of Canada's Constitutional System?' to mark with the 150th anniversary of the Canadian federation. My paper was published as 'Canada's Agonistic Constitution: Themes, Variations, Tensions, and Their On-Going Reconciliation' (2017) (2) ELTE Law Journal 13–30.

[4] Webber, Oliver Schmidtke, Eszter Bodnár, 'Special Issue: Democratic Constitutionalism in a Populist Age' (2023) 32 (6) Social and Legal Studies 841–995; Schmidtke, Webber Bodnár, 'The Resurgence of Populism: Tackling the Crisis of Liberal Democracy' (2021) 10 Social Sciences; Bodnár, Webber, Schmidtke, 'Populism, Democracy, and the Rule of Law in Central and Eastern Europe' (2024) 16 (2) Hague Journal on the Rule of Law 219–374.

I am only speaking about those populist parties that deserve our criticism, what might be called 'authoritarian populists', for some populists are simply boisterous democrats – when those populists that deserve our criticism are almost always also bad democrats, not merely disregarders of constitutions and the rule of law. And treating the rule of law as primarily a constraint on democracy is also a mistake professionally, for we neglect the ways in which the constitutional structures that foster democratic participation also tend to sustain healthy, law-respecting political orders. We emphasise the role of institutions that seek to constrain the actions of governments from (as it were) the outside – constitutional courts, for example – and neglect the development of the democratic institutions themselves, institutions that can foster more vibrant, more responsive, democratic orders.[5]

Why this tendency to see constitutionalism primarily in terms of constraint? I suspect that part of the reason is disciplinary specialisation. At least in Canada and the United States, there is a division of labour between legal scholars (who tend to focus on courts and adjudication) and political scientists (who tend to focus on legislatures and the executive). That division of labour is unexceptionable in its own terms, but it is unfortunate if it leads us to neglect the interconnections between the institutions.

But I think that there is also another contributing factor, and that is a growing loss of faith in democracy. I have been surprised by the number of my colleagues that have come to distrust democratic action. Some do so because they recognise, rightly, that our governments now face great challenges – climate change, for example – to which those governments have difficulty responding quickly and effectively. Others in North America seem to be shell-shocked by the rise of Donald Trump and his capture of the Republican Party, and they therefore seek to erect bulwarks against the depredations of another Trump-led government. In any case, there appears to be, among intellectuals, a growing worry that democratic government is unable to respond to the contemporary situation effectively, that the political decisions of our fellow citizens may even be a danger, and that we should therefore place our hopes in the action of constitutional courts, constraining, perhaps even directing, what governments ought to do.

That loss of faith is tragic and distressing. It is distressing because it risks abandoning what I take to be a central ideal of contemporary constitutionalism, namely the great merit, the dignity (to adopt Jeremy Waldron's term[6]), of collective, participatory self-government: the sense that the people ought to be able to govern themselves.[7] I have been

---

5 See Webber, 'A Democracy-Friendly Theory of the Rule of Law' (2024) 16 (2) Hague Journal on the Rule of Law 339–374. On populism generally, see Webber, 'Understanding Populism' (2023) 32 (6) Social and Legal Studies 849–876.

6 Jeremy Waldron, *The Dignity of Legislation* (Cambridge University Press 1999, Cambridge). On the general importance of taking disagreement seriously in legal theory, see Jeremy Waldron, *Law and Disagreement* (Oxford University Press 1999, New York).

7 See Webber, 'Democratic Decision Making as the First Principle of Contemporary Constitutionalism' in Richard W Bauman, Tsvi Kahana (eds), *The Least Examined Branch: The Role of Legislatures in the Constitutional State* (Cambridge University Press 2006, New York) 411–430.

blessed, throughout my career, by being able to work on Indigenous rights. There the central goal has been the freeing and rebuilding of Indigenous societies, re-empowered to govern themselves according to their own norms and procedures.[8] But have we, non-Indigenous scholars, championed Indigenous self-government only to lose faith in it for ourselves?

Moreover, the loss of faith in democracy is also distressing to the extent that it signals a loss of trust in our fellow citizens, a breakdown in our national conversations. Democracy is hard. It is hard precisely because democratic societies are diverse, democratic citizens disagree, and yet they also need to find ways to live and make decisions together. Democracy therefore requires work. It may not produce the decisions that we ourselves would make were we able to govern our societies alone. In fact, it is pretty much guaranteed not to produce those decisions precisely because, in a democracy, we do need to work together with people with whom we disagree. Yet that is also democracy's glory. Democracy allows us to maintain and express our own opinions. It allows us to disagree. And yet it also acknowledges that we are fated to live together, that we have to find some way to get along, and that we all are entitled to a say in how we do so. It recognises both our autonomy and our interdependence.

That does mean that democracy – that we – can fail. But even if we do fail, there is nevertheless a dignity in our entitlement to do so on our own responsibility and not have someone else do our failing for us. To be clear, I personally am hopeful of our capacity to succeed. Democracies, for all their frustrations, have proven remarkably resilient. Democracies won the Second World War, and they did so for reasons related to their democratic character.[9] The apparent solidity of the Communist-era autocracies proved

---

[8] See Webber, *Reimagining Canada: Language, Culture, Community and the Canadian Constitution* (McGill-Queen's University Press 1994, Montreal), especially 66–74, 111–115, 122–125, 170–172, 219–222; Webber, 'Individuality, Equality, and Difference: Justifications for a Parallel System of Aboriginal Justice' in Royal Commission on Aboriginal Peoples (ed), *Aboriginal Peoples and the Justice System: Report of the National Round Table on Aboriginal Justice Issues* (Minister of Supply and Services 1993, Ottawa) 133–160; Webber, 'Beyond Regret: *Mabo*'s Implications for Australian Constitutionalism' in Duncan Ivison, Paul Patton and Will Sanders, (eds), *Political Theory and the Rights of Indigenous Peoples* (Cambridge University Press 2000, Cambridge) 60–88; Webber, 'The Public-Law Dimension of Indigenous Property Rights' in Nigel Bankes, Timo Koivurova (eds), *The Proposed Nordic Saami Convention: National and International Dimensions of Indigenous Property Rights* (Hart 2013, Oxford) 79–102; Webber, 'We Are Still in the Age of Encounter: Section 35 and a Canada beyond Sovereignty' in Patrick Macklem and Douglas Sanderson (eds), *From Recognition to Reconciliation: Essays on the Constitutional Entrenchment of Aboriginal and Treaty Rights* (University of Toronto Press 2016, Toronto) 63–99; Webber, *Las gramáticas de la ley: Derecho, pluralismo y justicia* (Anthropos 2017, Barcelona, trans Francisco Beltrán Adell and Álvaro R. Córdova Flores); Webber, 'Governing Ourselves: Reflections on Reinvigorating Democracy Stimulated by Gitxsan Governance' in James Tully et al. (eds), *Democratic Multiplicity: Perceiving, Enacting and Integrating Democratic Diversity* (Cambridge University Press 2022, Cambridge) 281–303; Webber, *The Constitution of Canada: A Contextual Analysis* (2nd edn, Hart Publishing 2021, Oxford) at 209–247.

[9] This conclusion would doubtless be contested in the principal successor state to the USSR, Russia. The arguments to the contrary are convincing. See, for example, Phillips O'Brien, *How the War Was Won: Air-Sea Power and Allied Victory in World War II* (Cambridge University Press 2015, Cambridge). One need not make

temporary, as Hungarians above all demonstrated in 1989. And, despite all their claims, right-wing authoritarian governments have also proven remarkably fragile when viewed through the lens of history. In fact, they themselves confess their fragility, implicitly, through their strenuous attempts to muzzle their people and yet claim democratic authority. Why else would Putin's Russia have pretended to have its recent election?

But whether you share my (qualified) optimism or not, I cannot see a viable alternative but to cast our lot on the side of democracy, on the side of the dignity of collective self-government, and do our best within our scholarly disciplines to make democratic governance work. Legal institutions – even constitutional courts – depend upon their people's general support to sustain themselves. Indeed they depend upon, as I have argued and will argue, the mechanisms of democracy for their own integrity.[10] There is no alternative to engaging with our fellow citizens if we want to sustain healthy institutions. We are fated to live and govern ourselves, together.

We should, then, resist the temptation to adopt a predominantly defensive stance, looking to the courts to constrain what we might take to be excesses of democracy. Instead we should build our constitutionalism squarely upon democratic foundations, seeking to reinforce, not disable, the recursive, dialogic, participatory mechanisms of a vibrant democracy. In the rest of this lecture, I will describe in overview how the continued incorporation of democracy into the premises of our constitutionalism might shape our constitutional vision.

II Democracy

Let me start by saying a little more about what I mean by democracy.

Political and legal theorists often treat democracy as though it were simply about elections, perhaps about contested elections, sometimes about the alternation of governments as a result of elections. But a focus on elections or the alternation of governments misses the target. Putin's Russia has elections, but it is in no sense democratically governed. An election in which there is no real choice; in which opponents are disqualified, jailed, or worse; in which there is no media of communication that is independent of government; in which there is no real ability of citizens to know what their government is doing; and in which citizens have no basis for believing that their votes are being accurately counted –is not democratic. Russia is not an illiberal democracy. It is no democracy. The people are not allowed to rule. A corrupt, self-dealing, elite rules.

---

as far-reaching an argument as O'Brien's to establish that, without the productive power of the democracies, the USSR would not have succeeded in driving the Germans back. This is not, of course, to denigrate the fighting ability, fortitude, and sacrifices of the people of the USSR during the war.

[10] Webber, 'A Democracy-Friendly Theory of the Rule of Law' (n 5) at 354–367.

But it is also the case that elections are not absolutely necessary to have a democracy. One of my great privileges as a scholar has been the ability to see, up close, how one particular Indigenous people, the Gitxsan of northwestern British Columbia, govern themselves. I will not describe their subtle and elaborate governance structures at length, but suffice it to say that, in order to accomplish important legal transactions, they require careful consultation and preparation in advance, leading ultimately to the accomplishment of the legal operation itself in a feast, with structured opportunities for the attendees to express or withhold their approbation, in ways that are shaped by the patterns of membership and relationship within Gitxsan society. It does not require elections, but it does require participation, continuity of commitment, the public contribution of resources, and consultation. It is not easy. Indeed it is particularly demanding. But it is seen to be legitimate, tightly tied to the histories of Gitxsan houses (their *wilp*), their language, their principles, their relationships to territory, and their need to sustain themselves on their territory.[11]

Our experience of contemporary state-structured democracies, together with the Gitxsan example, therefore point to two characteristics that I take to be the essence of democracy. The first is the ability of a society's members to participate in their collective governance on a basis of rough equality, either directly or through representatives – and by participation I mean the exercise of some power to make decisions, by flesh-and-blood citizens, with respect to their governance, even if the effective power of any one citizen is diluted by the number of citizens entitled to participate. And lest one consider those requirements to be universal in form, necessarily the same for all societies, it is important to recognise that there is a second required characteristic of democracy, namely that the citizens ought to see themselves as being governed by processes that they themselves recognise as legitimate, institutions that are subject to their collective support, rooted in their societies – institutions that they, in a sense, 'own'.[12] As the legal theorist Nicole Roughan has argued in the context of Aotearoa/New Zealand, especially with respect to the application of New Zealand law to Maori, such recognition is essential. It is that sense of ownership that separates law from simple coercion.[13] It grounds the legal order in the

---

[11] Webber, 'Governing Ourselves' (n 8) and the sources cited there, especially Richard Daly, *Our Box Was Full: An Ethnography for the Delgamuukw Plaintiffs* (UBC Press 2005, Vancouver BC) 57–98; Val Napoleon, 'Living Together: Gitksan Legal Reasoning as a Foundation for Consent' in Jeremy Webber, Colin McLeod (eds), *Between Consenting Peoples: Political Community and the Meaning of Consent* (UBC Press 2010, Vancouver) 45–76.

[12] Webber, *Reimagining Canada* (n 8) especially 183–228; Webber, 'Individuality, Equality, and Difference' (n 8); Webber, 'The Meanings of Consent' in Webber, Macleod (eds), *Between Consenting Peoples* 3–41; Webber, 'Recognition in Its Place' in Daniel Weinstock, Jacob Levy and Jocelyn Maclure (eds), *Interpreting Modernity: Essays on the Work of Charles Taylor* (McGill-Queen's University Press 2020, Montreal) 247–264; Webber, 'A Nationalism Open Towards the World' in Rajeev Bhargava (ed), *Politics, Ethics and the Self: Re-reading Gandhi's Hind Swaraj* (Routledge 2022, New Delhi) 162–189.

[13] Nicole Roughan, 'Interlegality, Interdependence and Independence: Framing Relations of Tikanga and State Law in Aotearoa New Zealand' Appendix 3 to the study paper, He Poutama (NZLC SP24, 2023) (New Zealand:

people's traditions of governance. A true democracy can therefore take somewhat different forms in different societies, expressing the particular normative language of the society concerned.

In emphasising this two-part definition of democracy, in which elections are not essential to the definition, I do not mean to reject the mechanisms of electoral democracy as illegitimate. Some scholars do treat mechanisms as illegitimate, even as inauthentic, because elections substitute voting for the direct participation by citizens and subject even the votes that citizens cast to a complex process of summation and aggregation. I reject that view. For one thing, it is a dramatic oversimplification to reduce state-structured democracies to the casting of votes alone. States can and generally do provide other forms of participation alongside voting. But in addition, one cannot expect, in any real society, that discussion alone will resolve all disagreements. Even after full debate, members will still disagree, even over fundamentals, and those disagreements will need to be resolved by some additional means of decision. In a large-scale society, counting heads is a pretty good way to go. It has the great merit of *a)* actual means of participation for citizens, not merely an imputed or merely notional participation; and *b)* an institutionally-embodied norm of equality. Even in small-scale societies like the Gitxsan, one has mechanisms for sifting reasons and deciding outcomes in contexts of disagreement: one has processes for publicising the holding of feasts, those feasts are open to all comers, they provide for responses from the attendees that the work has been done properly, and in cases of dispute there are processes for weighing positions and fastening upon an outcome.[14] Indeed, some criticisms of mechanism strike me as dangerously romantic in their longing for unity. In attempting to achieve unity, they are likely merely to suppress the disagreements of their citizens.[15]

Moreover, in any large-scale society, even deliberation and decision will have to occur, in large part, through representatives. The only way one could avoid doing so is by restructuring societies so that they were very much smaller. Now, I do support decentralised government precisely to create greater opportunities for participation, but we also require the capacity for large-scale action – the kind of action that alone is capable of producing effective responses to climate change, providing better health care, achieving greater

---

Te Aka Matua o te Ture | Law Commission, 2023) <https://www.lawcom.govt.nz/assets/Publications/StudyPapers/NZLC-SP24-Appendix-3.pdf> accessed 15 October 2024.

[14] Webber, 'Democratic Decision Making as the First Principle' (n 7) at 418–422. On Gitxsan governance, see the sources cited (n 11).

[15] This of course is a central characteristic of the constitutional theory of Carl Schmitt and others on the anti-democratic right, although some on the left take comparable positions. See John P McCormick, *Carl Schmitt's Critique of Liberalism: Against Politics as Technology* (Cambridge University Press 1997, Cambridge); Webber, 'Understanding Populism' (n 5) at 853–857. For my position on Schmitt specifically see Webber, 'National Sovereignty, Migration, and the Tenuous Hold of International Legality: The Resurfacing (and Resubmersion?) of Carl Schmitt' in Oliver Schmidtke, Saime Ozcurumez (eds), *Of States, Rights, and Social Closure: Governing Migration and Citizenship* (Palgrave Macmillan 2008, New York) 61–90.

material equality and myriad other objectives. My conception of democracy is therefore federal, with a graduated structure of participation, representation and authority.[16]

We cannot, then, escape the construction of complex mechanisms of democratic governance. But keeping our focus on the two-part definition of democracy that I provided above – first, the ability of a society's members to participate in their collective governance on a basis of equality; second, their ability to 'own' those institutions – furnishes criteria for evaluating and therefore improving the mechanisms. A society's achievements will always be matters of degree. Any structure of participation will do some things well, some not so well. Moreover, there will always be variation in citizens' attachment to their institutions, both amongst elements within the citizenry and over time. The institutions themselves must therefore be open to reflexive redefinition. Democracy ought to operate both within the institutions as they exist from time to time, and control their evolution over time.

One last thing before I leave the question of definitions: When examining large-scale societies, the privileged expression of democratic legitimacy is almost always found in the legislature as opposed to the executive. This is because the legislature is larger and has a more diverse composition than the executive; it therefore serves as a better simulacrum of the people as a whole, capturing more accurately the range and balance of the citizenry. Moreover, the legislature's composition assists the democratic engagement of the citizenry because the openness of the chamber's processes, together with the continual presence of different segments of the population in those processes (especially the presence of the executive's opponents), furnishes a source of information on public affairs, a prominent position for questioning the government and holding it to account, and an effective stimulus to debate. Therefore, when I say that contemporary constitutionalism ought to focus more on enabling democratic governance than on constraining it, I will be referring primarily to how we as constitutional lawyers ought to approach the legislature. This accords with our historical experience. The great battles for advancing the rule of law focused on limiting arbitrary action by the executive, not on limiting democratic legislatures. Indeed historically, demands for strengthening the rule of law were allied with arguments for greater democratisation in the sense intended here. If one focuses, as I am doing, on democratic governance as a process – as the process of engagement of citizens in the decisions that will govern their lives – then the privileged institutional expression of that process will be the legislature.[17]

---

[16] Webber, 'Governing Ourselves' (n 8) at 298–302; Webber, 'Federalism's Radical Potential' (2020) 18 (4) International Journal of Constitutional Law 1324–1349.

[17] Webber, 'National Sovereignty, Migration, and the Tenuous Hold of International Legality' (n 15); Webber, 'A Democracy-Friendly Theory of the Rule of Law' (n 5) at 343.

III Features of Democratic Governance

So how, then, would this focus on the dignity of self-government reshape how we would characterise the chief features of a constitutional order?

We would continue to value certain rights as foundational to the existence of democracy. In addition to the expressly political rights – such as the right to vote – we would definitely include within this category freedom of speech and freedom of association, which are crucial to citizens' ability to formulate their opinions, develop evidence to support those opinions, express those opinions, build coalitions, and work to shape government policy. These are rights that are valuable not just within a citizen's private sphere but also as democratic rights – as rights of participation in the exercise of collective self-government.

Indeed, the rights' very importance to democratic engagement suggest their extension in ways that would not be true if their significance were limited to a private sphere. The need for rough equality in democratic participation means that they should be paired both with limitations on electoral spending (so those of great wealth do not control the political sphere) and with restrictions on media concentration (so that citizens have access to a diversity of information). Each of these measures expands the range of democratic engagement. They do not restrict it.

But in order to have effective participation, citizens also need to have access to information. They need to know what their governments are doing, they need to know what options their governments are considering, they need to know at what points they might be able to make representations. This requires openness in government and generous sharing of public-sector information – not merely disclosure upon special application but also the pro-active publication of data of public significance together with especially strong access for parliamentarians. Poorly-designed 'access to information' regimes can work against these goals by subjecting information to expensive and time-consuming applications, or by imposing limits on disclosure in order to protect private interests in a manner that is disproportionate to the public interests involved. The limitation of access to important public-sector contracts, in the supposed interest of commercial confidentiality, is an especially egregious example.[18]

There also need to be mechanisms that allow for the testing and assessment of this information. The disclosure of information has to include access to raw data so interpretations disseminated by governments can be verified. The existence of independent parliamentary officers, protected against retaliation, who can verify government accounts and institute safeguards against corruption is a further requirement. Moreover, there is good reason for knowledge to be held generally within society: for there to be independent

[18] Indeed, the impairment may be even more far-reaching than this suggests. Kristen Rundle argues convincingly that contracting-out can displace the foundational relationship of mutual responsibility between government and the citizenry: Kristen Rundle, 'Office and Contracting-Out: An Analysis' (2020) 70 (2) University of Toronto Law Journal 183–197.

universities, which can perform their autonomous analyses; for strong educational institutions throughout the country; for equality of access to education. What is more, here again, the existence of a diverse array of media serves democratic empowerment.

There also need to be structural opportunities for the people to know about and participate in the legislative process itself. This means a consistent process for the enactment of legislation, known to the public in advance, which allows for scrutiny, for response and for the making of representations.

An especially good way to encourage participation is to decentralise government – not just decentralising the delivery of services but also the making of public decisions, a decentralisation that might occur through (for example) the greater empowerment of provincial or municipal governments or the creation of specialist institutions (such as local tourism boards). Such initiatives provide accessible opportunities for participation in public decision-making, allow decisions to be adapted to local contexts, and create a ladder of opportunities that can lead to higher office. I began this lecture by noting a loss of faith in democracy. In my homeland, that loss of faith is a consequence, in some measure, of the erosion of forums in which people learn to work together despite their disagreements: non-governmental organisations, trade unions or boards that were once associated with public institutions. It is time that we sought to rebuild those important schools for democracy.

Finally, there need to be effective means for ensuring that the integrity of democratic decision-making is carried through to the moment of implementation. One of the eight components in Lon Fuller's influential statement of the rule of law is that there be congruence between declared rules and official actions.[19] That requirement is crucial to any truly democratic order. What use is democratic decision-making if it has little impact on what governments actually do? This is an additional reason for effective knowledge and scrutiny of government action. It is a good reason for structural mechanisms of oversight and accountability, and punishment when governmental actors behave corruptly. It requires protections for the independence of courts and prosecutors from government pressure. It emphasises the importance of a robust system of administrative law. All these things serve the constitutional objective of democratic government.

The above list is partial, suggesting the kind of reorientation inherent in a truly democratic constitutionalism. Note that the list does not limit or displace democratic decision-making. Instead, it enables it, helping to give it added force. The French political theorist Pierre Rosanvallon has demonstrated that the practice of democracy has always involved practices that go beyond participation in elections but which enable political argument and democratic decision-making to be responsive and informed. He calls these additional features 'contre-démocratie' – 'contre' in the sense of counterpoint, complementing and informing rather than contradicting.[20] Many of the elements in this list have that character.

---

[19] Lon L Fuller, *The Morality of Law* (2nd edn, Yale University Press 1969, New Haven) at 39 and 81ff.

[20] Pierre Rosanvallon, *La contre-démocratie: La politique à l'âge de la défiance* (Éditions du Seuil, 2006, Paris).

Not everything in the list would fall within the distinctive province of a lawyer, although a great many would do so. Indeed, several of the items would not be 'constitutional' in the sense in which that word is commonly used by legal scholars, yet they certainly serve as valuable foundations for effective democratic engagement – itself an argument for thinking about constitutionalism in ways that go beyond the strictly adjudicative. Moreover, we should never forget that lawyers do more than argue matters before courts. They also serve in constructive roles as legislative drafters, as designers of institutions, as administrators of regulatory regimes, as high officers within institutions, as policy analysts, as politicians themselves. Many perform roles in which this enabling of democratic agency would be acutely relevant. And it is also relevant in the heartland of the adjudicative role itself: in helping to articulate the interpretive frame within which strictly constitutional guarantees ought to be interpreted and applied.[21]

IV The People

Finally, the people, the citizenry – the *demos* in a democracy – has figured prominently throughout this argument. A democracy governs in the name of its people. But who constitutes that people? One characteristic of authoritarian populist movements is that they articulate a narrow and exclusive definition of the people.[22]

That tendency to narrow the political community is itself a problem. It often leads to a political culture prone to continual damaging schisms precisely because it fastens upon a set of characteristics that is much simpler than the lives that people actually live. If the criterion of membership is cultural, what happens when one of the movement's leaders marries someone from a foreign country? Is the marriage itself a sign of weakening loyalty? Are the children of that couple somehow less deserving of membership? Can they be full-fledged party members only if they give up one of their parents' languages? If the definition depends upon the rejection of 'gender ideology', must a true adherent choose between their nationhood and a daughter who enters into a same-sex relationship?

Moreover, that narrowing of the definition of people cheapens the nation itself, turning the nation into a caricature of itself.[23] Such definitions generally seek to freeze the nation in time, when any vigorous nation is always evolving, always extending its reach. Look back at definitions advanced by such movements 60 or 80 years ago. They now appear to be blinkered and deeply anachronistic. Moreover, any people is diverse politically and

---

[21] Webber, 'Constitutional Reticence' (2000) 25 Australian Journal of Legal Philosophy 125–155; Webber, 'A Modest (but Robust) Defence of Statutory Bills of Rights' in Tom Campbell, Jeffrey Goldsworth, Adrienne Stone (eds), *Human Rights Without a Bill of Rights: Institutional Performance and Reform in Australia* (Ashgate 2006, Aldershot) 263–287.

[22] Webber, 'Understanding Populism' (n 5) at 853–857.

[23] See Webber, *Reimagining Canada* (n 8) at 185–193.

culturally and that very diversity accounts for much of its dynamism. I come from a country in which much of its character is the result of the centuries-long interaction of French- and English-speaking societies. That interaction has created my country. It would not be the country I know had those two segments been separated. But of course I do not need to tell a Hungarian audience that. Hungary has not been well served by an exclusive, exclusionary nationalism. It is precisely that nationalism that is responsible for the fact that borders now separate them from so many of their cultural compatriots. And still today Hungary and those neighbouring societies are culturally diverse. Such diversity is the norm, not the exception.

Above all, a narrowing and exclusionary nationalism forfeits much of the justificatory force of democracy. Such a regime no longer governs in the name of all the people but in the name of a segment, a segment trying to impose its vision on other members of the people, advancing a kind of internal colonialism. A truly democratic constitutionalism treats its actual people, not its pretended people, as the custodians of its future, as the bearers of its political sovereignty.

That does not mean that such a country lacks a cultural character. Such a people still conduct its activities in a particular language or languages. In the case of Canada, that linguistic character is composite, drawing upon French, English, several immigrant cultures (including Hungarian) and increasingly (and belatedly) several Indigenous languages. Those components bring to the public life of the country the cultural resources carried by those languages, not least their distinctive literatures, their distinctive histories. Moreover, even within a single natural language – English for example – there are characteristics that are particular to each regional variant.[24] I am both Canadian and Australian, and even the English-language political cultures of my two countries are substantially different from one another. In Australia – which has refused to adopt a constitutionally entrenched bill of rights and which has a vigorous, one might even say populist political culture (populist mostly in the good democratic sense) – this argument for a democratic constitutionalism would be very easily made, perhaps even treated as old news, hardly worthy of an argument. And just as debates that occur within natural languages change over time, so the debates that occur within our political and legal cultures evolve and adapt and transform their societies through time. Any living people is not static, not a museum piece. Any of my Indigenous colleagues would tell you that.

Earlier in this lecture, my working definition of democracy treated, as one of its requirements, the members' recognition of the political structure as one appropriate for their collective self-government. That element draws our attention to this cultural dimension of nationhood – a dimension that need not be exclusive or reactionary, but that can be confident and inclusive.

---

[24] Webber, *Reimagining Canada* (n 8) especially 222–226; Webber, 'A Nationalism Open Towards the World' (n 12).

V Conclusion

I began this lecture by thanking you for giving me the opportunity to renew my engagement with the struggle to establish freedom, democracy, self-government, in a distinctively Hungarian democratic and constitutional order. Each country's trajectory is unique, each is instructive, each holds lessons that are unique to that context but instructive to others.

My thanks to you. My thanks to Eötvös Loránd University. Let us all continue to learn and to grow into a fuller understanding of the requirements of a truly democratic constitutionalism.

Symposium

Gergely Gosztonyi*

Preface to the Contributions on Digital Authoritarianism, Internet Fragmentation, Splinternet, Censorship and Cyber Sovereignty

The divergence between cyber libertarianism and cyber paternalism characterised discussion related to internet governance in the 1990s. Decisions on content regulation issues were settled in the United States of America (US) with the Communication Decency Act Section 230 and in Europe with the notice-and-takedown system of the E-commerce Directive. However, the era of privatised freedom of expression faced challenges from the mid-twentieth century onwards, from Christchurch and troll farms to the Cambridge Analytica scandal. For a few years now, internet regulation has been a vital issue on the political agenda in all parts of the world, characterised in the US by the need to amend CDA230 and the 'dragging' of giant tech mammoths' leaders before the Senate. In the European Union (EU), the process led to the adoption of the Digital Services Act (DSA) – Digital Markets Act (DMA) – and European Media Freedom Act (EMFA) package of regulations. Meanwhile, for example, in China, the process of change is characterised by the ongoing development of the Golden Shield and the Great Firewall based on the concept of cyber sovereignty, and in Russia, by the wish to disconnect from the international internet network. The increasingly undemocratic practices of these latter rogue states may be attractive to many other countries, and such solutions have started being exported.

Alas, there is a global trend towards governments increasingly resorting to internet restrictions, often for illegitimate purposes and with disproportionate impacts on the public. This shift in international norms towards greater government intervention in the digital sphere is a matter of urgent concern. Technical and legal solutions can range from denying user access through filtering technologies and unlawful bandwidth throttling to collateral and excessive and wholesale blocking by states. This trend necessitates urgent attention and action.

* Dr Gergely Gosztonyi PhD, Habil. Associate Professor, Eötvös Loránd University (ELTE), Faculty of Law. ORCID iD: 0000-0002-6551-1536.
The whole volume on digital authoritarianism, internet fragmentation, splinternet, censorship and cyber sovereignty was supported by the project no. 149657 which has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the ADVANCED_24 funding scheme.

Thus, scholarly articles about cyber sovereignty and its legislation are crucial due to the intricate and evolving nature of internet governance and its profound implications for global politics, security, and individual freedoms. Cyber sovereignty, a concept that refers to a state's right to govern and control internet activity within its borders, is gaining prominence as nations face increasing cyber threats. The Center for Strategic and International Studies (CSIS) reports that the global cost of cybercrime will reach $10.5 trillion annually by 2025. Researching and documenting how different countries enforce cyber sovereignty provides critical data on the effectiveness of various policies.

The legislative landscape of cyber sovereignty varies widely, with over 120 countries having enacted cybersecurity laws by 2023, according to the United Nations Conference on Trade and Development (UNCTAD). These laws range from comprehensive data protection regulations, such as the European Union's General Data Protection Regulation (GDPR), to more fragmented and sector-specific approaches seen in countries around the globe. According to Freedom House's 2023 report, approximately 70% of internet users live in countries where governments impose significant censorship or surveillance. In Asia, countries like China and North Korea enforce strict internet censorship.

Similarly, Russia's Sovereign Internet law aims to route internet traffic through state-controlled infrastructure, increasing the government's ability to control and monitor online activities. Countries like South Korea and Japan have more open internet policies but enforce significant regulations. Examining these practices can provide a nuanced understanding of the trade-offs between national security and individual freedoms, generating data-driven recommendations that support the implementation of balanced approaches.

The role of international human rights courts in dealing with cyber sovereignty and internet restrictions cases is increasingly significant. These courts recognise the implications of such issues on human rights and have ruled on several cases involving state surveillance and internet censorship. For instance, the European Court of Human Rights (ECtHR) has addressed state surveillance and internet censorship, while the Inter-American Court of Human Rights (IACtHR) has highlighted the illegal interception of communications.

Of critical importance is that research on cyber sovereignty and related legislation cannot be accomplished without analysing the technical details and infrastructure behind the internet. This way, addressing the global shortage of cybersecurity professionals would help meet this challenge. In Asia, countries such as Singapore and India invest heavily in cybersecurity education and training to build a workforce capable of addressing emerging threats. Europe is also proactive, with initiatives like the European Cybersecurity Skills Framework (ECSF) intended to enhance cyber education and professional development across the EU. Data shows that countries with solid cybersecurity education programs, such as Israel, have higher employment rates in the cybersecurity sector and better job performance outcomes. Integrating academic research into training and professional development will ensure that the next generation of experts is well-equipped to holistically navigate the complex landscape of cyber sovereignty and internet governance.

Fourteen scholars from ten countries have gathered to discuss those crucial issues concerning modern communication. In the first part of this issue of the ELTE Law Journal, Dorina Gyetván paints a general picture, showing that online private censorship is no longer just a theoretical distant possibility but an everyday reality. Carmen Moldovan highlights the conflict between the idea of state control over the internet and the impact on freedom of expression and access to information, as well as the challenges of the state-driven regulatory model. Adelina-Maria Tudurachi asks if Internet access could or should be seen as a fundamental human right, examining the relevant case law of the European Court of Human Rights and the Court of Justice of the European Union (CJEU). Gergely Ferenc Lendvai focuses on the right to access the Internet (RATI) as seen by the ECtHR and finds it in great danger in Russia and Turkey. Xiaojuan Grace Yang has created a comprehensive overview of World Internet Conferences and China's promotion of cyber sovereignty, giving details about a less well-researched and known topic.

The second part of this ELTE Law Journal issue deals with the European online media legislation processes. Boris Kandov writes about the DSA, clearly underlining that it introduces several new regulations concerning algorithm-based, automatic filtering systems into EU law that are playing a significant role in online platforms, as algorithms are used there in the form of filtering and recommendation systems. Simona Veleva anticipates the challenges with the regulatory implementation of the DSA into national regulatory frameworks; the article focuses on the harmonisation process and the challenges posed by different legal traditions and regulatory approaches.

Readers may swim in the ocean of more technical questions in the third part of this issue of the ELTE Law Journal. Tuba Eldem thoroughly shows how the Internet is increasingly becoming a domain of control, surveillance, and regulation by states and private entities. The article investigates Web3 architecture in relation to countering sovereign controls with a mixed-method approach that synthesises insights from computer science, political science, and legal studies. Roland Kelemen, Joseph Squillace, Richárd Németh and Justice Cappella investigate the relationship between the United Nations Sustainable Development Goals and Internet access, focusing on how digital connectivity influences the achievement of these global objectives and revealing that a robust IT identity enhances digital inclusion and empowerment. In the last article, Ádám Farkas and László Vikman examine information operations as a question of law and cyber sovereignty, reviewing different nation-state solutions and providing a conceptual framework that incorporates legal, political, military and intelligence aspects.

On this basis, the articles in this issue of the ELTE Law Journal examine governmental and other policies and actions that constrain or prevent the use of the Internet to create, distribute, or access information. As a Guest Editor of the ELTE Law Journal, I hope to foster a more comprehensive and detailed understanding of censorship and internet content restrictions by bringing diverse perspectives and expertise together. This is, perhaps, a small contribution to the long fight against digital authoritarianism.

Dorina Gyetván*

Censorship and Freedom of Expression in the Age of Social Media

Abstract

Although social media platforms have altered the structure of the public sphere, they have also inherited some of its issues, notably the problem of censorship. The phenomenon has remained, just its methods and practices have changed: censorship used to be strictly connected to states, but in the digital age, it is exercised by multiple actors, such as states, private companies and individuals (users), posing a unique and multilevel threat to freedom of expression. Social media service providers are motivated by their own economic interests and pressured by vague laws that impose liability for third-party user content; the combination of these factors steers service providers to ignore human rights standards, err on the side of caution, and tend to remove, block or restrict any questionable content in order to avoid liability. Therefore, online freedom of expression faces problems, just as it did in offline formats in analogue times, and often even more severe ones. However, technological advances mean that new censorship methods often remain unperceived by users and, therefore, often avoid the harsh criticism surrounding traditional censorship. In 2020, Facebook (Meta) set up the Oversight Board, a uniquely positioned semi-independent expert group as a sort of court-like body to deal with some of the more high-profile, influential and complex social-media-related decisions and offer a remedy against contract-based content moderation (censorship).

Keywords: freedom of expression, censorship, Oversight Board, flooding, content moderation

I Preamble

Social media platforms have fundamentally altered the structure of the public sphere, allowing masses of people to post their opinions, learn about the opinions of others,

* Dr Dorina Gyetván, PhD Candidate, ELTE Doctoral School of Law. ORCID iD: 0000-0001-5361-0011.

and share other's expressions.[1] At the beginning of the Internet's rise, the latter was put on a pedestal as the ultimate embodiment of freedom, equality and total freedom from censorship. Given the above characteristics, it was perceived as almost inconceivable that any state could control and restrict the flow of information.[2] On the one hand, one could simply conclude that 'new media were born to be free, although, inevitably, they are not a lawless domain, they do not tolerate any censorship or authority, the main reason being that media cannot be controlled by the state due to the technological nature thereof'.[3] Although the method, motive, scope and effectiveness of content moderation on the Internet varies from state to state, it initially seemed like social media platforms would allow users to break free from the traditional 'top-to-bottom' nature of state power.[4]

However, '[...] the control of information on the Internet and Web is certainly feasible, and technological advances do not therefore guarantee greater freedom of speech. There are many tools available and still more in development.'[5] Therefore, the Internet is not inherently distinct from the traditional media world and has inherited many of its problems as well.[6] In fact, transforming previously existing restrictions and combining them with advanced technological tools creates a brand new environment for arbitrary state intervention while simultaneously allowing private service providers to intervene arbitrarily. The early phenomena of decentralisation and complete lack of regulation are continuously declining. Power is increasingly concentrated in the hands of a few influential service providers; the growing economic power and the unstoppable development of technology have brought about overbearing censorship in the online space, similar to the censorship of traditional mass communication.

The aim of this paper is to take the traditional phenomenon of censorship as a starting point and investigate online freedom of expression as mainly controlled by modern social media service providers, to outline the new forms of censorship, and to briefly discuss the significance of intermediary service provider liability in this context, and the possible role of

---

1 Dirk Voorhoof, Hannes Cannie, 'Freedom of Expression and Information in a Democratic Society. The Added but Fragile Value of the European Convention on Human Rights' (2010) 72 (4–5) International Communication Gazette, DOI: https://doi.org/10.1177/1748048510362711

2 Gabriella Szabó, 'Internetes portálok médiaszociológiai és politológiai elemzése' (2008) 17 (4) Politikatudományi Szemle 62–63; Judit Oszti, *Az elektronikus média szerepe korunk háborúinak társadalmi-politikai megítélésében és a közgondolkodás formálásában* (Zrínyi Miklós Nemzetvédelmi Egyetem 2009, Budapest) 25.

3 László Majtényi, Gábor Polyák, 'A szabadság hazai hagyományának megtagadása – új médiatörvények Magyarországon' (2011) 4 (1) Közjogi Szemle 4; András Koltay, 'Az internet mint médium, a sajtószabadság és a demokratikus nyilvánosság' (2014) 14 (4) Információs Társadalom 16, DOI: https://doi.org/10.22503/inftars.XIV.2014.4.1

4 Márton Iványi, 'Az online közösségi hálózatok és a véleménynyilvánítás pozitív és negatív szabadsága' (2015) 25 (3) Iskolakultúra 82, DOI: https://doi.org/10.17543/ISKKULT.2015.3.72

5 William H. Dutton and others, *Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet* (UNESCO Publishing 2011, Paris).

6 Koltay (n 3) 16.

the Oversight Board concerning the extent to which such an entity is able to counterbalance the shortcomings of content moderation (private censorship).

II Traditional Censorship in the Narrow Sense

Censorship is as old as mankind itself. The Old Testament showed how Jeremiah was condemned to death for criticising the leaders of the people and prophesying against Judah.[7] Censorship of certain forbidden subjects was also common practice in ancient Greece; for example, the Greek philosopher Socrates was condemned to death for his teachings in 399 BC. In the analogue age, the term 'censorship' originally referred to state intervention in the content published in media, which proved to be an effective tool prior to the digital age,[8] as all (most) major communication outlets involved some kind of centralised state control, and the prospect of severe punishment was sufficiently discouraging to instil fear in citizens due to its draconian rigour.

What is obvious is that censorship was primarily linked to the state as the embodiment of concentrated power. In the age of modern technology, however, the concept should be more broadly interpreted and generally used in a wider sense:[9] we should not only understand censorship to refer to restrictions imposed by the state(s) but also to encompass the ability and inclination of social media service providers, which are gaining power by the minute, to restrict content on the basis of their private, financially motivated interests, which, over time, encourages the presence of so-called self-censorship on an ever wider scale as a result of external and internal moral convictions.[10]

III Modern Censorship

It might seem sensible to simply argue that social media providers cannot censor, as they are private entities, and only the state has the authority to censor.[11] However, to avoid the looming liability posed by national and international laws, service providers have taken a number of steps towards enacting more extensive regulations, such as hiring whole armies of moderators, adopting and enforcing private (contractual) rules, and developing a wide

---

7 Bible. *Old Testament*. Jeremiah 26.

8 John Naughton, 'How China censors the net: by making sure there's too much information' (2018) The Guardian, <https://www.theguardian.com/commentisfree/2018/jun/16/how-china-censors-internet-information> accessed 15 October 2024.

9 Gergely Gosztonyi, 'A cenzúra tipizálása a politikai cenzúra rövid történetének tükrében' (2022) 23 (1) Médiakutató.

10 András Koltay, 'A médiatartalmak közzététel előtti korlátozásának lehetőségei: engedélyezés, regisztráció, cenzúra, végzések' (2014) 10 (1) Iustum Aequum Salutare 77.

11 Amitai Etzioni, 'Should We Privatize Censorship?' (2019) 36 (1) Issues in Science and Technology 19.

variety of algorithm-based solutions. One of the main drawbacks of such control is the lack of legitimacy and accountability behind the decisions of private entities, mainly due to a (total) lack of transparency.[12] One thing that is for sure, however, is that the rise of social media services has triggered a heated and ongoing debate about how these platforms moderate the content published, shared, or generated by users on their platforms. In light of the above, Jack M. Balkin's 'new school'[13] of speech regulation can be described by three determining features:

1. collateral censorship;
2. the intertwining of the operations of public and private service providers; and
3. global private regulation.[14]

The algorithmic society has also multiplied the entities that are able to restrict freedom of expression; the digital age has brought about a 'pluralist model of speech governance',[15] so that the user can now expect intervention by the state and private entities, either through indirect censorship imposed by state coercion or due to the service providers' own economic interests. Social media has the power to shape and change public opinion, and the decisions of social media service providers determine who can participate in online public discourse and to what extent. Such characteristics are very similar to the phenomenon of traditional censorship.

Censorship in the digital age and censorship in the traditional sense certainly have one thing in common: they both threaten freedom of expression.[16] However, a significant difference, which makes the phenomenon of private censorship an even more significant issue, is that while traditional media censorship is typically confined to geographical boundaries such as state or administrative borders, in the age of the Internet, it is increasingly common to see more extensive, worldwide restrictions on freedom of expression.

From New Zealand[17] to the United States of America,[18] social media has often been at the centre of attention due to the repercussions of numerous tragedies. Therefore, the obligations, liabilities and responsibilities of service providers seem to be drifting further and further away from the initial solution of awarding them full immunity. In addition to the obvious positive effects of social media, we also perceive that the provision of unprecedented

---

12 Haggart, Blayne, Keller, Clara Iglesias, 'Democratic legitimacy in global platform governance' (2021) 45 (6) Telecommunications Policy 2, DOI: https://doi.org/10.1016/j.telpol.2021.102152

13 Jack M. Balkin, 'Free speech in the algorithmic society. The new school of big data, private regulation and the regulation of expression' (2018) 118 (7) Columbia Law Review 1173.

14 Balkin (n 13) 1176.

15 Balkin (n 13) 1186.

16 Iványi (n 4) 83.

17 'Mészárlás Új-Zélandon: vészforgatókönyvet vett elő a YouTube' (2019) HVG, <https://hvg.hu/tudomany/20190319_uj_zeland_meszarlas_tomeggyilkossag_facebook_elo_video> accessed 15 October 2024.

18 Teddy Wayne, 'The Trauma of Violent News on the Internet' (2016) The New York Times, <https://www.nytimes.com/2016/09/11/fashion/the-trauma-of-violent-news-on-the-internet.html> accessed 15 October 2024.

publicity cannot (and does not) exist without limits: social media service providers, with their power, technological capabilities and position, also assist in silencing the opinions of users. Social media service providers are in their heyday. The phenomenon of private censorship is a recurrent problem, as one of the main issues is that service providers' content-related decisions are (partly) rooted in their own economic interests, often without a legal basis. They are fully or partially made by employing artificial intelligence, lacking transparency, guarantees and even the possibility of effective remedy (appeal).[19]

IV New Forms of Censorship

In recent years, more sophisticated methods have been deployed by service providers, so new methods of regulating and restricting freedom of expression other than traditional censorship have emerged. These show great variety, but the common ground is that their emergence is ultimately somehow linked to the rise of private service providers:

1. self-censorship has become even more prominent with the emergence of service providers;
2. reverse censorship has emerged, involving controlling public opinion by flooding the information space using private operators;
3. collateral censorship refers to the phenomenon whereby states use their power over social media providers to encourage moderation by imposing the principle of secondary liability.

1 Self-censorship

Censorship is usually only discussed in the context whereby one entity restricts another individual's expression.[20] However, one manifestation of indirect censorship is self-censorship, which refers to the phenomenon whereby individuals such as social media users 'voluntarily' act in ways that eliminate the need for a censor.

Within the category of self-censorship, we can distinguish between public and private self-censorship.[21] In the case of public self-censorship, we refer to the situation when the censor is a government or a public authority, the restricted person is a natural person or legal

[19] Thiago Dias Oliva, 'Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression' (2020) 20 (4) Human Rights Law Review 612, DOI: https://doi.org/10.1093/hrlr/ngaa032

[20] Paul Sturges, 'Self-Censorship: Why We Do the Censors' Work For Them' (2008) LIBCOM Conference, 2, <https://www.ifla.org/wp-content/uploads/2019/05/assets/faife/publications/sturges/self-censorship.pdf> accessed 15 October 2024.

[21] Philip Cook, Conrad Heilmann, 'Two Types of Self-Censorship: Public and Private' (2013) 61 (1) Political Studies 179, DOI: https://doi.org/10.1111/j.1467-9248.2012.00957.x

entity, and the latter resorts to self-censorship because of looming sanctions or prior filters imposed by external entities. Such pressures may include, for example:

1. a compelling reason related to the owner of the service provider;
2. ex-post liability; or
3. prior restrictions such as licensing procedures or any kind of approval.[22]

Public self-censorship means that individuals internalise certain aspects of public censorship and then censor themselves.[23] The indirect result of the public sphere's 'intervention' is thus the abandonment of one's true wilful expression: ie, unwanted voluntary – and by voluntary, I mean here the absence of actual direct, external intervention – self-censorship without involving any legal dispute or potential costs. Through such indirect pressure, content potentially generating controversy will be removed from social media without any tangible intervention.[24] In contrast to public self-censorship, private self-censorship is, in fact, an internal self-regulatory process involving an irreconcilable antagonism between what an individual considers publicly permissible to express and what one actually wishes to express publicly.[25]

From the above, it is clear that the distinction between the two types of self-censorship is based on whether the censor and the restricted person are united in one or two distinct entities: in the case of public self-censorship, the censor is a separate entity from the individual, whereas, in case of private self-censorship, the censor and the restricted are the same person, thus we refer to the suppression of one's own attitudes.[26]

Self-censorship has become an even more significant threat to freedom of expression since the emergence of intermediary service providers, as the failure to express one's views on the platforms with the largest audiences cannot be replaced by expressing one's self on other, less popular platforms.[27] This is also why multiple, simultaneous censors are particularly threatening to freedom of expression (as much as certain codes of conduct or other contractual provisions are) – namely, because external regulators (ie, those other than state law or international law) can have such a chilling effect on users through their vague wording and lack of procedural guarantees against arbitrary decisions that it leads to self-censorship.[28]

---

22 Sturges (n 20).

23 Cook, Heilmann (n 21) 179.

24 András Koltay, *A szólásszabadság alapvonalai* (Századvég Kiadó 2009, Budapest) 202.

25 Cook, Heilmann (n 21) 179.

26 Cook, Heilmann (n 21) 194.

27 András Koltay, 'Szólásszabadság, avagy a social media jogi státusa – 5. rész' (2019) Jogászvilág, <https://jogaszvilag.hu/szakma/szolasszabadsag-avagy-a-social-media-jogi-statusa-5-resz> accessed 15 October 2024; János Tamás Papp, 'Recontextualizing the Role of Social Media in the Formation of Filter Bubbles' (2023) 11 (1) Hungarian Yearbook of International Law and European Law 136–150, DOI: https://doi.org/10.5553/HYIEL/266627012023011001012

28 Koltay (n 27).

2 Reverse Censorship

The phenomenon of what Eugene Volokh calls 'cheap speech' refers to the fact that, with the development of technology, anyone can form an opinion on any issue and distribute it for free (or at least without significant cost).[29] This opportunity is no longer limited to those who can navigate the decisions and expectations or prescriptions of old gatekeepers: '[t]oday we live in an environment where speech is cheap, where it is abundant, where the fundamental challenge is no longer finding speakers but rather finding attention for speech'.[30]

Perhaps no one would argue that censorship has a long history in China, but the rise of social media platforms is generating more than 30 billion different pieces of content every day,[31] a volume of content that has made control over public discourse an unimaginably complex task.[32] There are three possible ways to effectively control the floods of information on the Internet: by fear, causing traction, and flooding.[33] Causing fear is far too costly and can easily backfire by generating significant resistance due to social media's potential. This reverse outcome is often referred to as the 'Streisand effect' in the literature – the fact that attempts to hide certain information can often end up attracting more public attention to whatever the actor (here, the state) was initially trying to hide.[34] Therefore, Chinese media typically uses one of three methods – the Great Firewall, keyword blocking or flooding – to regulate online content, the latter of which is distinct from the censorship tendencies of any other state.[35]

Flooding,[36] which refers to the collective and structured method of disseminating masses of information,[37] is not about removing undesirable content as quickly as possible or imposing liability on the person responsible for the expression in question, but an approach designed to distract and eliminate the threat inherent in the power of the community and volume of information.[38] The flooding method is more economical and no less effective

---

29 Eugene Volokh, 'Cheap Speech and What It Will Do' (1995) 104 (7) Yale Law Journal 1805, 1849, DOI: https://doi.org/10.2307/797032

30 David A. Graham, 'The Age of Reverse Censorship' *The Atlantic*, 2018, <https://www.theatlantic.com/politics/archive/2018/06/is-the-first-amendment-obsolete/563762> accessed 15 October 2024.

31 Naughton (n 8).

32 Graham (n 30).

33 Margaret Earling Roberts, *Fear, Friction, and Flooding: Methods of Online Information Control* (Harvard University 2014, Cambridge, Massachusetts) 91.

34 Sue Curry Jansen, Brian Martin, 'The Streisand Effect and Censorship Backfire' (2015) 9 (1) International Journal of Communication 666.

35 Gergely Gosztonyi, 'Special models of internet and content regulation in China and Russia' (2021) 9 (2) ELTE Law Journal 87–99, DOI: https://doi.org/10.54148/ELTELJ.2021.2.87

36 Roberts (n 33) 32–33.

37 Roberts (n 33) 91.

38 Gary King, Jennifer Pan, Margaret Earling Roberts, 'Reverse-engineering censorship in China: Randomized experimentation and participant observation' (2014) 345 (6199) Science 1251722, DOI: https://doi.org/10.1126/science.1251722

than traditional censorship. This approach has the added advantage of being able to control community discourse through 'the most targeted suppression of expression'[39] while avoiding the outrage associated with direct censorship.[40]

3 Collateral Censorship – Content Moderation or Censorship?

The term 'collateral censorship' was first coined by Michael I. Meyerson[41] to refer to the situation when states target the transmitter of the opinion (eg, the social media service provider) in order to restrict the actual (primary) author of the expression, ie, the user. Cheap speech on the Internet is made possible by intermediary service providers, but the same service providers can potentially and arbitrarily silence expression as well.[42] Moreover, these technological giants are more in the public eye and easier to identify than users who communicate under pseudonyms or hide behind the veil of anonymity.[43]

Furthermore, with the technological solutions at the social media service providers' disposal, it is clearly more practical for states to encourage them to regulate online expression than directly restrict the users who are the actual authors of the expression. The prospect of holding intermediary service providers liable generates a chilling effect that can (and in practice does) incentivise them to 'over-block' content.[44] The latter, sometimes without distinction, also remove legitimate content from the public discourse if it is problematic (even slightly or seemingly controversial) simply to avoid being held liable.[45]

Private regulation (censorship) by service providers involves the drafting, enforcement and detection of breaches of community standards and other contractual provisions. During the course of such procedures, intermediary service providers monitor and make decisions about the permissibility of the online content (expression) uploaded by everyday users on the basis of contractual provisions with the assistance of automated and human resources that lack a proper legal basis, since the removal, blocking and other restrictions are usually not based on hard law but internal contractual provisions and semi-transparent standards and codes.

The root of the problem, beyond the fact that service providers do not act according to human rights standards, is that they tend to choose to err on the side of caution and

---

39 Gary King, 'Reverse Engineering Chinese Censorship' (2014) Talk at ESRC Research Methods Festival, 5.

40 Roberts (n 33) 41.

41 Michael I. Meyerson, 'Authors, Editors, and Uncommon Carriers: Identifying the "Speaker" Within the New Media' (1995) 71 (1) Notre Dame Law Review 116.

42 Felix T. Wu, 'Collateral Censorship and the Limits of Intermediary Immunity' (2013) 87 (1) Notre Dame Law Review 299.

43 Wu (n 42) 300.

44 Sheera Frenkel, 'Facebook Says It Deleted 865 Million Posts, Mostly Spam' (2018) The New York Times <https://www.nytimes.com/2018/05/15/technology/facebook-removal-posts-fake-accounts.html> accessed 15 October 2024.

45 Wu (n 42) 300.

remove, block or otherwise restrict any questionable content to avoid liability. However, the distinction between lawful and unlawful content is often not clear-cut; it cannot be made on the basis of preset criteria without exploring and understanding the expression's context. Accordingly, much lawful content and many lawful users fall victim to the moderation practices of social media service providers.[46]

V Intermediary Service Provider Liability and the Prohibition of a General Monitoring Obligation according to the ECD and the DSA

To reduce the risks and occurrence of collateral censorship described above, the European Union provides varying degrees of immunity for intermediary service providers depending on their type.[47] Prior to the Digital Services Act (DSA),[48] the regulatory framework for EU digital services was primarily based on the E-Commerce Directive (ECD).[49] As part of the EU legislation, it provided safe harbour immunity under certain conditions specified in Articles 12–14. However, this legislation is not able to prevent the evils of collateral censorship since the ECD does not eliminate private censorship due to its permissive and vague provisions. In fact, the ECD explicitly encouraged service providers to deploy private censorship.[50] Such permissive and encouraging wording was intended to be counterbalanced by the prohibition on imposing a general obligation of monitoring in Article 15, which would effectively amount to Internet censorship.[51] Article 15 explicitly prohibits the imposition of general monitoring obligations with regard to due diligence proceedings on intermediary service providers, ie, the general obligation to detect and prevent illegal content on their platforms.[52]

However, the ECD did not define the meaning of the term 'general monitoring', thereby creating undesirable uncertainties as to how this prohibition (limitation) should

---

46 Wu (n 42) 301.

47 Andrea Kovács, 'A közvetítő szolgáltatások meghatározásának egyes problémáiról' in Gergely Gosztonyi (ed), *A velünk élő történelmi cenzúra* (Gondolat Kiadó 2022, Budapest) 85–96.

48 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

49 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1.

50 ECD Article 12(3), Article 13(2) and Article 14(3).

51 Ádám Liber, 'A közvetítő szolgáltatók felelőssége a szellemi tulajdon megsértéséért az Európai Unióban' (2013) 118 (3) Iparjogvédelmi és Szerzői Jogi Szemle 31.

52 Martin Senftleben, Christina Angelopoulos, *The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market* (University of Amsterdam – University of Cambridge 2020, Amsterdam – Cambridge) 6.

be interpreted in relation to intermediary service providers. The findings in the case law of international forums,[53] which also encourage service providers to use automatic mechanisms to avoid liability for third-party content, may also be problematic from the point of view of fundamental rights as automatic solutions such as various algorithm-based filtering or ranking mechanisms are not able to adequately interpret the context of the content in question[54] and thus have a chilling effect on freedom of expression.

In 2020, the European Commission officially presented the DSA proposal as part of a comprehensive digital strategy, and certain provisions concerning the largest platforms became applicable at the end of August 2023.[55] The regulation has been applicable in its entirety since 17 February 2024.[56] The DSA sought to define a uniform set of conditions for all service providers in relation to their exemption from liability and due diligence obligations; however, to avoid disproportionality in the case of smaller service providers, the DSA also applies asymmetric regulation to smaller actors on the market.[57] Even though, as a regulation, the DSA is a set of directly applicable rules that now apply to digital services across the EU, the DSA further confirms[58] the prohibition of general monitoring defined in Article 15(1) of the ECD with the provision remaining relatively unchanged, preserving the previous notice-and-takedown-system (coined as a notice and action mechanism in the DSA). Recital 30 of the DSA indicates that monitoring obligations in specific cases would not be counter to the prohibition defined in Article 8 of the DSA: intermediary service providers should not be, either *de jure* or *de facto*, subject to a monitoring obligation with respect to obligations of a general nature (general active fact-finding obligation, or as a general obligation for providers to take proactive measures in relation to illegal content),[59] but this does not concern monitoring obligations in specific cases and, in particular, does not affect orders by national authorities in accordance with national legislation in compliance with Union law, as interpreted by the Court of Justice of the European Union, and in accordance

---

53 Gergely Gosztonyi, *Censorship from Plato to Social Media. The Complexity of Social Media's Content Regulation and Moderation Practices* (Springer 2023, Cham), 121– 145, DOI: https://doi.org/10.1007/978-3-031-46529-1_9

54 Giancarlo Frosio, Sunimal Mendis, 'Monitoring and Filtering: European Reform or Global Trend?' in Giancarlo Forsio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2019, Oxford) 21. DOI: https://doi.org/10.1093/oxfordhb/9780198837138.013.28

55 Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (2024) 38 (3) Berkeley Technology Law Journal 883–920, DOI: https://doi.org/10.2139/ssrn.4598426

56 DSA Article 93.

57 European Commission: Questions and answers on the Digital Services Act, 23 February 2024. <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348> accessed 15 October 2024.

58 DSA Article 8.

59 Herbert Zech, 'General and specific monitoring obligations in the Digital Services Act' (2021) Verfassungsblog, 2021 <https://verfassungsblog.de/power-dsa-dma-07> accessed 15 October 2024, DOI: https://doi.org/10.17176/20210902-113002-0

with the conditions established in the DSA.[60] As we can see, however, similarly to the preceding ECD, the legislator does not specify what would constitute a specific case.[61] Furthermore, one may find a so-called 'Good Samaritan' clause in the DSA, which stipulates that service providers are not to be held liable if they, in good faith and in a diligent manner, voluntarily carry out own-initiative investigations into or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content, or implement the measures necessary to comply with the requirements of Union law and national law in compliance with Union law, including the requirements set out in the DSA.[62]

Article 8 would only be an appropriate provision capable of stopping the proliferation of collateral censorship if the distinction between specific and general monitoring obligations were clearly defined and general monitoring was not necessary for exemption from liability.[63] The courts' insistence on maintaining the general-individual distinction is not without reason: the difference is not merely based on economic or proportionality reasons, but rather it is designed to act as a guarantee: 'by exerting pressure and imposing responsibility on those who control the technological infrastructure, [governments] create an environment in which [...] censorship of private partners is an inevitable result'.[64]

VI Is the Oversight Board Able to Counterbalance the Shortcomings of Private Censorship?

The Oversight Board is a 26-member expert group[65] set up by Facebook (Meta) to independently review some of the most difficult and significant content-related decisions of Facebook, Instagram and Threads. It is sometimes referred to as Facebook's 'Supreme Court'.[66] On the one hand, when users have exhausted the relevant platform's appeals process concerning the aforementioned services, they may challenge the latest decision about a piece of content by appealing to the Oversight Board; on the other hand, Meta may

---

60 Valentina Golunova, 'In Tech we Trust? Fixing the Evolutionary Interpretation by the Court of Justice of the Prohibition of General Monitoring in the Era of Automated Content Moderation' in Evangelia Psychogiopoulou, Susana de la Sierra (eds), *Digital Media Governance and Supranational Courts: Selected Issues and Insights from the European Judiciary* (Edward Elgar Publishing 2022, Cheltenham) 62.

61 Gergely Gosztonyi, Andrej Skolkay, Ewa Galewska, Challenges of Monitoring Obligations in the European Union's Digital Services Act. (2024) 12 (1) ELTE Law Journal, DOI: https://doi.org/10.54148/ELTELJ.2024.1.45

62 DSA Article 7.

63 Anupam Chander, 'When the Digital Services Act Goes Global' (2023) 38 (4) Berkeley Technology Law Journal, DOI: https://doi.org/10.15779/Z38RX93F48

64 Frosio, Mendis (n 54) 16; *Delfi AS v Estonia,* no. 64569/09 (ECHR, 16 June 2015), Joint Dissenting Opinion of Judges Sajó And Tsotsoria 17.

65 Oversight Board: Updates On Oversight Board Membership (2023) <https://www.oversightboard.com/news/771690787717546-updates-on-oversight-board-membership/> accessed 15 October 2024.

66 Tamás Pongó, 'Új korszak az online véleménynyilvánítás korlátozásában? Gondolatok a Facebook Oversight Board működéséről' (2020) 4 (147) Iustum Aequum Salutare.

also refer issues to the Board.[67] The Oversight Board started accepting cases in the Autumn of 2020. The main objective of such an experimental body was to oversee the platform's decisions and provide guidance on what content should or might be removed, what should be left online, and why. In other words, it is an ongoing experimental attempt to remedy the harm caused by private censorship.

Without going into the details of the functioning or the content of the Oversight Board's decisions in this paper,[68] I will simply highlight a few key characteristics that underpin or, on the contrary, confirm or refute the Board's ability to counteract the anomalies described in the previous sections of this paper.

With regard to the potential of the Oversight Board, in its almost four years of operation, it has generated a number of benefits that represent a positive step forward for the exercise of freedom of expression online. Based on its track record, it is safe to say that its relevance extends beyond the adjudication of individual cases, and its aim is to establish a precedent system over time that provides a human rights-based, fast and flexible forum[69] for users to challenge the platform's content decisions. In addition to specific decisions, it provides further guidance[70] for the platform to act more in line with human rights standards and laws in the future. By meticulously selecting complex cases, it can also serve as a guide and benchmark for other decisions on probably more straightforward issues, thus impacting the platform's processes significantly more than just deciding individual cases.

However, there are still many areas where the Board lacks real influence that could potentially, with certain improvements, provide real, significant solutions to the problem of private censorship. Despite initial efforts, it does not function as an independent body; it is inseparable from the platform in a number of crucial ways.[71] There are also procedural safeguarding concerns, such as the anonymity of the committee members who decide on individual cases, the lack of due diligence due to the tight deadlines for procedures and the fact that human rights considerations are secondary to 'lex Facebook',[72] which the procedure is primarily based on. The various limitations of the respective procedures are a further concern in terms of the number of cases actually picked out for examination, the decision-making concerning the caseload and demand, and the strict requirements for eligibility to initiate proceedings.[73]

---

67 Oversight Board Charter Article 2, Section 1.

68 Cf: Gergely Ferenc Lendvai, 'A Facebook Ellenőrző Bizottság működése és bíráskodása a gyűlöletbeszéd kontextusában' (2024) 13 (1) In Medias Res, DOI: https://doi.org/10.59851/imr.13.1.11

69 Oversight Board, Bylaws Article 2, Section 2.

70 Oversight Board, Bylaws Article 2 Section 2 and Article 1 Section 4.

71 Oversight Board, Bylaws Article 1, Section 1.1.2., Article 2, Section 1.3.1.

72 Lorenzo Gradoni, 'Constitutional Review via Facebook's Oversight Board' (2021) Verfassungsblog, <https://verfassungsblog.de/fob-marbury-v-madison> accessed 15 October 2024, DOI: https://doi.org/10.17176/20210210-235949-0

73 Rebecca Heilweil, 'You can finally ask Facebook's oversight board to remove bad posts. Here's how' (2021) Vox, <https://www.vox.com/recode/22381607/facebook-oversight-board-appeal-remove-post-ads> accessed 15 October 2024.

In terms of the effectiveness of the available legal remedy, access is of decisive importance, and based on this criteria, the Oversight Board, from the point of view of average users, lacks potential: the Board has complete discretion as to which matters it deliberates and adopt a decision on. As of July of 2024, the Board has only delivered 107 decisions,[74] while during the course of its operation until Q2 of 2023 more than 2.7 million cases were submitted[75] to it. This means that only 0.004% of the cases submitted to the Board have been actually decided by the Board. The various jurisdictional limits, such as restrictions on the type of explicit content (eg, spam), the type of decision (eg, decisions concerning intellectual property), and certain services (eg, Messenger),[76] severely limit users' ability to submit cases to the Board and completely exclude the possibility of review in many cases.

The Oversight Board can, in its binding decisions, instruct Facebook to remove or keep certain content intact and online, as well as to amend its decisions, which the platform is obliged to implement within seven days. In fact, according to Section 4 of the Articles of Association, Facebook is required to search for content identical to the content affected by the decision and apply the same procedure as was the subject of the original decision if the necessary technological tools and organisational resources are available.[77] This can be compared to the emerging trend related to the prohibition of general monitoring obligations,[78] according to which platforms are expected not only to take certain steps in the event of specifically contested matters but to search for specific harmful content that occurs in the same context and act against this as well.

VII Conclusion

On the one hand, social media has given people unprecedented opportunities and a unique platform to express their opinions and receive information, but it has also transformed the institution of censorship that was established during the era of traditional media.

Censorship was once concentrated in the hands of states, but now, in the social media age, the role of the censor has been partially taken over by a number of private entities with economic power and technological tools, which arbitrarily define the limits of freedom of expression. The state's desire to restrict social discourse has not ceased, but how it is achieved has been transformed. This has resulted in a system in which a number of (new) actors have emerged (alongside the actual person expressing their opinion) that, on the one hand, are able and keen on restricting freedom of expression and, on the other, forced to

[74] See <https://transparency.meta.com/oversight/oversight-board-cases> accessed 15 October 2024.
[75] Oversight Board, 2023 Q2 Transparency Report.
[76] Oversight Board, Bylaws Article 2, Section 1.2.1.
[77] Oversight Board, Bylaws Article 1, Section 2.3.1.
[78] Senftleben, Angelopoulos (n 52).

cooperate in unprecedented ways, thus increasing the presence of censorship as a threat to freedom of expression. Instead of the single bipolarity of relationships that used to exist regarding traditional media, there is now a complex network of multiple actors that threaten freedom of expression, either directly or indirectly (private censorship of platform providers and public self-censorship) or through reverse censorship. What these different methods of restriction have in common, however, is that they can be identified as new 21st-century forms of censorship, as they are likely to involve the deliberate and systematic curtailment of fundamental rights such as freedom of expression guaranteed by law, driven by the opaque, unforeseeable, arbitrary economic and other interests of a private company or multiple private companies.[79]

Accordingly, today, private censorship is no longer just a theoretical distant possibility; it is a reality in our everyday lives. Social media service providers themselves have the ability and means to decide about any content on their platforms, but they are dangerous actors in relation to states in an age when traditional censorship methods no longer provide sufficient solutions to limit freedom of expression.[80] The combination of these factors creates a new situation for democratic discourse and forums – an environment in which freedom of expression can be restricted by multiple actors, driven by a great variety of motives, often without any or at least without sufficient procedural safeguards, and mainly (especially in the case of flooding) without being perceived by the actual author of the expression, thus posing an unprecedented threat to freedom of expression.

[79] Gábor Megadja and others, *A Facebook-cenzúra ellen* (Századvég 2019, Budapest) 42.

[80] Folkert Wilman, 'Two emerging principles of EU internet law: A comparative analysis of the prohibitions of general data retention and general monitoring obligations' (2022) 46 (1) Computer Law & Security Review, DOI: https://doi.org/10.1016/j.clsr.2022.105728

Carmen Moldovan*

Mirror, Mirror on the Wall, Who's the Most Authoritative of Them All? Cyber Sovereignty from a Critical Perspective

Abstract

The paper aims to highlight the conflict between the idea of state control over the Internet and the impact on freedom of expression and access to information and to challenge the state-driven regulatory model. The doctrine of cyber sovereignty, as advocated by China and Russia, is an example of such control in the absence of international legally binding regulation. First, the special features of cyberspace as a *sui generis* phenomenon are presented, as well as the attempts of the United Nations to create a legal framework for this special environment. Second, the digital perspective of the right to access information is analysed, followed by the meaning of the principle of state sovereignty and the impact on the digital space, especially its fragmentation. Addressing this conflict is crucial to safeguarding fundamental rights in the digital empire, divided between the doctrine of human rights, the idea of open space and the control of information supported by authoritative regimes.

Keywords: cyberspace, digital environment, access to information, state control

I Introduction

The development of the Internet has had a profound impact on technology and communications, influencing and advancing human activity at many levels and establishing cyberspace as a global ecosystem that would not be possible in its absence. The creation of a digital empire with special features generates multiple problems related to the identification of applicable rules, the extent of the protection of fundamental rights and the balance of power, including new dimensions for international law.[1]

* Dr Carmen Moldovan PhD, Associate Professor, Alexandru Ioan Cuza University of Iasi, Faculty of Law. ORCID iD: 0009-0002-7470-8557.

1 Philip Alston, Colin Gillespie, 'Global Human Rights Monitoring, New Technologies, and the Politics of Information' (2012) 23 (4) The European Journal of International Law 1089–1123

Cyberspace has been characterised as being chaotic, anarchic[2] and asymmetric with respect to resources and capabilities[3] in order to justify the notion of state cyber sovereignty that safeguards the latter's best interests as they relate to other states; establishing this principle does not resolve all of the subsequent difficulties such as state responsibility and repercussions concerning the interests and rights of private individuals and non-state actors.[4]

The concept of cyber sovereignty is referred to as the establishment and control of a 'national cyberspace'[5] subject to domestic laws, authoritarian in nature, with the goal of seizing complete control of cyberspace and the Internet and isolating them from the global network, which contradicts the very essence of their existence. Although such an idea is presented as an alternative to the intention of the United States to build a hegemonic order in global cyberspace[6] and as a means of ensuring the principle of equality between states, taking into consideration that there are significant differences in actual access to cyberspace due to unequal technological levels of development, the outcome is a fragmented environment that negatively affects fundamental rights, especially freedom of expression and access to information. Such a submission disregards the fact that, in practice, cyber sovereignty only widens the gap between technologically advanced nations and developing ones. On the contrary, a free and global cyberspace offers open accessibility to public information and the public sector to everyone. Thus, employing such arguments plainly shows that the issue of cyber standards continues to be a tool of geopolitical rivalry.[7]

DOI: https://doi.org/10.1093/ejil/chs073; Daniel Bethlehem, 'The End of Geography: The Changing Nature of the International System and the Challenge to International Law' (2014) 25 (1) The European Journal of International Law 9–24. DOI: https://doi.org/10.1093/ejil/chu003

2 Séverine Arsène, 'Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order?' (2016) (2) China Perspectives 28, DOI: https://doi.org/10.4000/chinaperspectives.6973; Jinghan Zeng, Tim Stevens, Yaru Chen, 'China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"' (2017) 45 (3) Politics & Policy 451, DOI: https://doi.org/10.1111/polp.12202

3 Yi Shen, 'Cyber Sovereignty and the Governance of Global Cyberspace' (2016) 1 Chinese Political Science Review 84, DOI: https://doi.org/10.1007/s41111-016-0002-6

4 Issues linked to the topic of cyber sovereignty have been analysed previously by the author: Carmen Moldovan, 'On the normative equivalence paradigm in cyberspace' 177 02002 (2023) SHS Web of Conferences Legal Perspectives on the Internet. COPEJI 6.0, DOI: https://doi.org/10.1051/shsconf/202317702002; Carmen Moldovan, 'Suveranitatea digitală – viitorul spațiului virtual? (2021) 67 (2) Analele Ştiinţifice ale Universităţii Alexandru Ioan Cuza din Iași Științe Juridice 271–284, DOI: https://doi.org/10.47743/jss-2021-67-4-19

5 Milton Mueller, *Sovereignty and Cyberspace: Institutions and Internet governance,* Essay presented at the 5th Annual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana October 3rd 2018 <http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/10410/5th-Ostrom-lecture-DLC.pdf?sequence=1&isAllowed=y> accessed 15 October 2024.

6 Yi Shen (n 3) 82; Daniel Joyce, 'Internet Freedom and Human Rights' (2015) 26 (2) The European Journal of International Law 494–514, DOI: https://doi.org/10.1093/ejil/chv021

7 Harriet Moynihan, 'Power Politics Could Impede Progress on Responsible Regulation of Cyberspace' (2019) <https://www.chathamhouse.org/expert/comment/power-politics-could-impede-progress-responsible-regulation-cyberspace> accessed 15 October 2024.

Although relatively intriguing, the idea that various types of cyberspace or virtual frontiers may be established by governments according to their interests and supported by territorial sovereignty has ramifications for other regulations and rules. The term cyber sovereignty may be considered inaccurate or a misnomer simply because the principle of sovereignty, which is the cornerstone of international law, cannot be fully transferred to this environment. The notion of territorial sovereignty in cyberspace must be applied in a restrictive manner and only in relation to elements of Information and Communication Technology (ICT) infrastructure on state territory, as it results from the conclusions of special groups established with the purpose of identifying how international law applies in the digital empire and not impacting on freedom of expression.

II Cyberspace – From Matrix to a *Sui Generis* Phenomenon

States appear to be unable to reach a consensus on how to govern cyberspace or even how to comprehend how this intricate ecosystem works. Since the goal of international law is to regulate state behaviour within cyberspace rather than the environment itself, discussing its characteristics may be helpful in addressing the conflict between the legal concept of sovereignty and this environment, as well as the implications for free speech.

Terms used to refer to cyberspace[8] are inconsistent and synonymously include 'virtual space', 'digital space', and 'digital ecosystem'.[9] Instead of being utilised or defined as such under international law, the United Nations prefers to use the term 'Information and Communication Technology' (ICT) in various reports and documents. Cyberspace is one of the greatest of humanity's creations; it does not rely on natural elements; it is entirely human-made[10] and is a complex global network, a logical space which is unlimited, imperceptible, non-materialised, time-dependent[11] and constantly changing. It is an interconnected information system which has been developed by non-state actors and has

[8] The term was coined by William Gibson in his cyberpunk book *Neuromancer* (Ace Books 1984): 'Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts… A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.'

[9] Eileen Donahoe, 'The Need for a Paradigm Shift on Digital Security' in Fen Osler Hampson, Michael Sulmeyer, (eds), *Getting beyond Norms New Approaches to International Cyber Security Challenges* (Special Report, Centre for International Governance Innovation 2017) 31.

[10] Marie Baezner, Patrice Robin, *Trend Analysis: Cyber Sovereignty* (Risk and Resilience Team Center for Security Studies 2018, ETH Zürich) 8.

[11] Rain Ottis, Peeter Lorents, 'Cyberspace: Definition and Implications' in Leigh Armistead (ed), *Proceedings of the 5th International Conference on Information Warfare and Security* (Academic Conferences Limited 2010, Reading) 267.

no borders[12] corresponding to physical territory. This is entirely opposed to state territory, which has a material and physical dimension, yet cyberspace requires the physical support of material infrastructure.[13] Employing the expression 'Information Society'[14] is adequate with reference to the components of freedom of expression.

Currently, cyberspace is being used for a variety of activities and purposes, including military operations. Its special traits make it a *sui generis* phenomenon[15] that challenges rules and principles already established and widely recognised. Although it may not be the subject of exclusive state control, its features are no longer sufficient to qualify as *res communis omnium*,[16] excluding all forms of sovereignty[17] similar to the high seas or outer space.

III The Complicated Relationship between International Law and Cyberspace

1 From an Unregulated Environment to (Blurred) Normative Equivalence

The absence of a legal definition of cyberspace serves as the foundation for any form of activity by states and may impact their responsibility to protect fundamental rights. There are no legally enforceable mechanisms governing this environment, despite the fact that states and other stakeholders[18] (including employees, shareholders, marketers, mass media organisations, civil society groups, and, in general, platform users)[19] have expressed concern and even proposed regulations. The task of developing and clarifying cyber standards is

12 Katrin Nyman Metcalf, 'Legal View on Outer Space and Cyberspace: Similarities and Differences' Tallinn Paper 2018/10, 2.

13 Yi Shen (n 3) 83.

14 Daniel Joyce, 'Internet Freedom and Human Rights' (2015) 26 (2) The European Journal of International Law 493–514, DOI: https://doi.org/10.1093/ejil/chv021

15 Dennis Broeders, Liisi Adamson, Rogier Creemers, 'Coalition of the unwilling? Chinese and Russian perspectives on cyberspace' (2019) The Hague Program For Cyber Norms Policy Brief 2, <https://www.thehaguecybernorms.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace> accessed 15 October 2024.

16 Wolff Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' in C. Czosseck, R. Ottis, K. Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict* (NATO CCDCOE Publications 2012, Tallinn) 8.

17 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press 2012, Oxford) 203.

18 Anri van der Spuy, *What if we all governed the Internet? Advancing multistakeholder participation in Internet governance* (UNESCO Series on Internet Freedom 2017, Paris) 26.

19 Barrie Sander, 'Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law' (2021) 32 (1) European Journal of International Law 166, DOI: https://doi.org/10.1093/ejil/chab022

not just the responsibility of the United Nations. The contribution of regional bodies and organisations is equally essential.

In general, regional instruments are limited in scope, and they do not specify what it means by the 'responsible behaviour of states' in this regard. The Budapest Convention on Cybercrime[20] and its Additional Protocol[21] define a restricted scope for the criminal activity of individuals using information systems that does not address jurisdiction issues. The Shanghai Organisation (headed by Russia and China) in its International Information Security Agreement[22] defines cyber warfare but does not address other aspects of state action or applicable standards of international law.

In 2015, the Shanghai Organisation presented the International Code for Information,[23] which received little attention or reaction from other states. The International Code for Information Security is intriguing in terms of terminology;[24] at least in part, the goal of this code of conduct is similar to the suggestions created by the United Nations. It refers to the United Nations Charter, specifically to the principles of sovereignty, territorial integrity and political independence.[25] Overall, it refers to the general application of international law, which may apply to states' cyber conduct and, as opposed to other texts, the Code focuses on information society[26] rather than cybersecurity. However, it only serves a declaratory purpose.

The Tallinn Manual 2.0 on International Law Applicable to Cyber Operations (The Tallinn Manual 2.0)[27] is widely regarded as the most comprehensive academic work on the

---

[20] *Convention on Cybercrime*, opened for signature 23 November, 2001 ETS 185 (entered into force on 1 July 2004).

[21] *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* opened for signature 28 January 2003, ETS 189.

[22] *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security*, Yekaterinburg, 16 June 2009 <https://eng.sectsco.org/documents/?year=2009> accessed 15 October 2024.

[23] Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, sixty-ninth session Agenda item 91 Developments in the field of information and telecommunications in the context of international security, UN Doc A/69/723 <https://ccdcoe.org/uploads/2018/11/UN-150113-CodeOfConduct.pdf> accessed 15 October 2024.

[24] It provides that its purpose is 'to identify the rights and responsibilities of States in the information space, promote constructive and responsible behaviour on their part and enhance their cooperation in addressing common threats and challenges in the information space, in order to establish an information environment that is peaceful, secure, open and founded on cooperation, and to ensure that the use of information and communications technologies and information and communications networks facilitates the comprehensive economic and social development and well-being of peoples, and does not run counter to the objective of ensuring international peace and security', International Code of Conduct, § 1.

[25] International Code of Conduct, § 2(1).

[26] Broeders, Adamson, Creemers (n 15) 2.

[27] Michael N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017, Cambridge) DOI: https://doi.org/10.1017/9781316822524

subject of cyber activities. It offers useful content about the concepts of sovereignty and non-intervention in cyberspace, but it does not provide answers to all questions and concentrates on themes such as the use of force in peacetime, preventative self-defence, cyber-attacks and determining the imminence of cyber-attacks. In chapter 2, the concept of state sovereignty in cyberspace is examined in relation to the physical aspects of state infrastructure[28] located on their territory. Although not legally binding, the Tallinn Manual had a significant impact on state cyber activity.[29] Version 3 is now awaited.[30] There are also various private initiatives aimed at establishing cyberspace rules.[31]

2 The Findings of the United Nations on Sovereignty in Cyberspace

Currently, it is commonly agreed that international law applies to cyber operations,[32] resolving previous disputes and refuting the claim that states should refrain from regulating this field as a means to protect Internet freedom. One legal implication of this acknowledgement is that states are required to abide by corresponding rights and obligations in their cyberspace activities,[33] including ensuring the safeguarding of fundamental freedoms.

Soft law tools, such as reports from specialised United Nations working groups like the UN Group of Government Experts (the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

---

[28] The terms are the following: '[a] State enjoys sovereign authority with regard to cyber infrastructure… located within its territory', Schmitt (n 27) 13.

[29] Michael N. Schmitt, Liis Vihul, 'The Nature of International Law Cyber Norms' Tallinn Paper 2014/5, 31.

[30] <https://ccdcoe.org/research/tallinn-manual/> accessed 15 October 2024.

[31] The Paris Call for Trust and Security in Cyberspace was launched in 2018 as a multistakeholder initiative and formulated nine principles (<https://pariscall.international/en/> accessed 15 October 2024). Principle number 9 refers to international norms, and it aims to promote the widespread acceptance and implementation of international norms of responsible behaviour as well as confidence-building measures in cyberspace. A Digital Geneva Convention was proposed by Microsoft in 2017, and it underlines the importance of international humanitarian law in cyberspace without giving details on how this is applicable and to what extent. It is at the same time appreciated [Joseph Guay, Lisa Rudnick, 'What the Digital Geneva Convention means for the future of humanitarian action' (25 June, 2017) The Policy Lab <https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/> accessed 15 October 2024] and criticised [Valentin Jeutner, 'The Digital Geneva Convention. A Critical Appraisal of Microsoft's Proposal', (2019) 10 (1) Journal of International Humanitarian Legal Studies 158–170, DOI: https://doi.org/10.1163/18781527-01001009].

[32] Maria Tolppa, 'Overview of the UN OEWG developments: continuation of discussions on how International Law applies in cyberspace' (2020) <https://ccdcoe.org/library/publications/overview-of-un-oewg-developments-continuation-of-discussions-on-how-international-law-applies-in-cyberspace/> accessed 15 October 2024.

[33] Antonio Coco, Talita de Souza Dias '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law' (2021) 32 (3) The European Journal of International Law 771–805, DOI: https://doi.org/10.1093/ejil/chab056; Sean Kanuck, 'Sovereign Discourse on Cyber Conflict' (2010) 88 Texas Law Review 1575.

– UNGGE) and the Open-ended Working Group (OEWG),[34] emphasise the voluntary nature of non-binding norms, rules and principles governing responsible state behaviour in cyberspace. These reports support the use of international law in cyberspace and call for confidence-building measures to increase trust between states and strengthen global cybersecurity. Despite being among the first UN endeavours on the subject,[35] these reports fall short of providing clear direction for implementing these ideas or developing customary international law.

The common thread across all legal frameworks concerning state activities in cyberspace is the acknowledgement that existing international law provides the foundation for regulating states' conduct.[36] However, none of these reports delineate specific implementation strategies, nor do they constitute elements of international customary law. State practice remains varied or involves silence, notwithstanding the latter's authority to formally adopt rules governing conduct in cyberspace. To advance clarity on the application of international law to cyber sovereignty, a strategic shift may be necessary, separating discussions on this specific issue from broader political deliberations on behavioural norms and confidence-building measures.[37]

The UN GGE, established in 2004,[38] represents a significant step towards identifying cyber norms and addressing responsible state behaviour in cyberspace. Critical to its work are the 2013[39] and 2015 reports that assert that UN Charter principles extend to states' conduct and operations in cyberspace. Notably, both Russia and China participated in this group.

---

[34] United Nations Office for Disarmament Affairs, Fact Sheet – Developments in the field of information and telecommunications in the context of International Security (July 2019) <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf> accessed 15 October 2024.

[35] Tolppa (n 32).

[36] Moynihan (n 7).

[37] François Delerue 'The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?' (2018) 7 (4) European Society of International Law Reflections 2.

[38] United Nations Office for Disarmament Affairs 2019. Initially, it was established as an exclusive body, with 15 members (Belarus, Brazil, China, France, Germany, India, Jordan, Malaysia, Mali, Mexico, Russia, South Africa, South Korea, United Kingdom, United States of America). The numbers expanded to 25 for the period 2004–2005 (Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States, and Uruguay).

[39] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Developments in the field of information and telecommunications in the context of international security-Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' Sixty-eighth session Agenda item 94, U.N. Doc. A/68/98 (24 June 2013) § 19.

The 2013 report emphasises the application of state sovereignty to ICT-related activities and jurisdiction over ICT infrastructure within state territories,[40] albeit with some ambiguity regarding an open ICT environment versus state sovereignty in ICT matters.

Similarly, the 2015 Report[41] reaffirms the principles of international law outlined in the previous report and the application of sovereignty[42] and provides recommendations,[43] albeit without providing clearer insights. Referring to infrastructure does not actually solve the problem because this has a mixed or hybrid character determined by the influence of private companies and is part of a global network.[44]

Despite these efforts, the UN GGE faced challenges, culminating in a deadlock in 2017 due to disagreements over the right to self-defence and the applicability of international humanitarian law to cyber conflicts.[45] Subsequently, the UN established the OEWG in 2018,[46] which operated more inclusively,[47] allowing all interested UN member states to participate. However, like its predecessor, the OEWG failed to provide clear guidance on the application of international law to cyberspace and its work ended in 2021.

Critically, the findings of these reports, while significant, remain limited[48] considering their soft law[49] nature. They highlight the lack of consensus about the application of international law, reflecting the politically influenced nature of these working groups.[50] Despite the impasse, it is essential to recognise that the failure to reach a consensus and

---

40 The wording of the Report is the following: 'State sovereignty and the international norms and principles that flow from it apply to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure with their territory'. A/68/98 § 20., 27., 28.

41 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 17th sess item 93 of the provisional agenda UNGA UN Doc A/70/174 (22 July 2015).

42 UN Doc A/70/174, § 13(h), §§ 24., 26.

43 Paul Meyer, 'Norms of Responsible State Behaviour in Cyberspace' in Markus Christen, Bert Gordijn, Michele Loi (eds), *The Ethics of Cybersecurity* (Springer 2020) 353, DOI: https://doi.org/10.1007/978-3-030-29053-5_18

44 Dimitri Van Den Meerssche, 'Compressing All Data into Actionable Risk Scores': The Construction of Virtual Borders' (2022) 33 (1) The European Journal of International Law 176, DOI: https://doi.org/10.1093/ejil/chac007; Thomas Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 (4) The European Journal of International Law 799–839, DOI: https://doi.org/10.1093/ejil/chn040

45 Stefan Soesanto, Fosca D'Incau, 'The UN GGE is dead: Time to fall forward. Commentary' (2017) <https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance> accessed 15 October 2024.

46 Developments in the field of information and telecommunications in the context of international security GA Res 73/27 UN Doc A/RES/73/27 (5 December 2018).

47 Tolppa (n 32).

48 Bruno Lété, Peter Chase, 'Shaping Responsible State Behavior in Cyberspace' (2018) The German Marshall Fund of the United States Workshop Briefing Paper 6.

49 Dinah Shekton, 'International Law and Relative Normativity' in Malcolm D. Evans (ed), *International Law* (Oxford University Press 2014, Oxford) 159.

50 Soesanto, D'Incau (n 45).

adopt cyber norms[51] does not equate to an unregulated cyberspace. Instead, it highlights the complexities and challenges inherent in governing this dynamic domain.

The primary legal implication of the existence only of soft norms or quasi-norms[52] is that breaching obligations does not involve international responsibility for states, as outlined in the Draft Articles on State Responsibility,[53] and does not trigger identical legal remedies. Typically, a breach of an international obligation involves restitution.[54] When applied to cyber operations, if a state's cyber activity breaches another state's sovereignty, the affected state would theoretically be entitled to restitution, but this remains an unresolved issue. The ongoing reinterpretation of existing norms and rules in this domain may prove crucial in the future formulation of regulations applicable to states in cyberspace. The International Court of Justice's *Advisory Opinion on Namibia* may be significant in this regard as it states that an 'international instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of interpretation'.

IV The Cyber Right to Access Information

Access to information as a part of the right to freedom of expression is guaranteed by several international law instruments in similar terms. These include Article 19 of the Universal Declaration of Human Rights[55] and the International Covenant on Civil and Political Rights (hereinafter ICCR),[56] Article 10 of the European Convention on Human Rights,[57] Article 13 of the Inter-American Convention on Human Rights,[58] Article 9 of the African Charter of Human and Peoples' Rights.[59] It constitutes a topic of interest for the UN from different perspectives[60] and for regional organisations.

---

51 Tim Maurer, 'A Dose of Realism: The Contestation and Politics of Cyber Norms' (2020) 12 (2) Hague Journal on the Rule of Law 285, DOI: https://doi.org/10.1007/s40803-019-00129-8

52 Toni Erskine, Madeline Carr, 'Beyond 'Quasi-Norms: The Challenges and Potential of Engaging with Norms in Cyberspace in Anna-Maria Osula, Henry Rõigas (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCDCOE Publications 2016, Tallinn) 100.

53 Responsibility of States for Internationally Wrongful Acts, GA Res 56/83, UN GAOR, 56th sess, 85th plen mtg, Supp No 49, UN Doc A/RES/56/83 (28 January 2022, adopted 12 December 2001).

54 *The Factory at Chorzow* (Germany v Poland) (Claim for Indemnity) (The Merits) [1927] PCIJ (ser A) No 13, 28.

55 *Universal Declaration of Human Rights* (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR).

56 *International Covenant on Civil and Political Rights* opened for signature 19 December 1966, 999 UNTS 171 (ICCPR).

57 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force on 3 September 1953).

58 *American Convention on Human Rights*, opened for signature 22 November 1969, 123 UNTS 1144 (entered into force 18 July 1978).

59 *African Charter on Human and Peoples' Rights*, opened for signature 27 June 1981, 217 UNTS 1520, (entered into force 21 October 1986).

60 Eneken Tikk, Mika Kerttunen, *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, (Cyber Policy Institute 2017) 14.

The scope of freedom of expression and of the right to receive and impart information and ideas is similar in all international legal instruments. For the purpose of this paper, only the provisions of Article 19 of the Universal Declaration on Human Rights and of ICCPR will be analysed. The Universal Declaration provides that 'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers'. Article 19 of the ICCPR has similar wording and also mentions the requirements that the states must comply with when interfering with its exercise.

Creating a national cyberspace under the full control of the state cannot be considered a legitimate restriction in the sense of paragraph 3 of Article 19. When applying restrictions to freedom of expression, states must comply with their obligations provided by international instruments. China only signed the ICCPR in 1998 and did not ratify it. The Russian Federation signed the Covenant in 1968 and ratified it in 1973.[61] According to Article 2, paragraph 1 of the ICCPR, states have a negative and a positive obligation to ensure rights are recognised. This means that restrictions must be permissible and must prove their necessity and proportionality in pursuing a legitimate aim.[62]

As already mentioned, cyberspace is an environment characterised by communication and the transfer of data and information, which could not have been envisaged by the drafters of all international instruments that regulate freedom of opinion and access to information. However, all of them have a common feature: the safeguards of the freedom of expression and access to information are recognised regardless of frontiers.

The Human Rights Council has stressed that 'the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights'.[63] And at the same time, it 'recognizes the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms; and calls upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries.[64] The UN Human Rights Council reiterated these conclusions in 2014, and they are at the moment generally accepted. Previously, the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion

[61] <https://indicators.ohchr.org/> accessed 15 October 2024.

[62] Human Rights Committee, *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant* (2004), adopted by the Human Rights Committee at the 80th sess, CCPR/C/21/Rev.1/Add.13 (29 March 2004) § 5., 6., 8.

[63] Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, 26th sess Agenda item 3 UN Doc A/HRC/20/L.13 (29 June 2012).

[64] UN Doc A/HRC/20/L.13.

and expression,[65] Frank La Rue, underlined the implications of the Internet for the freedom of expression and access to information.

Also, at the universal level, UNESCO has engaged in assiduous activity, usually by cooperating with other entities to support Internet freedom and access to information. It is not the purpose of this paper to analyse these works, yet some of them are particularly relevant, taking into consideration the moment they were adopted and their divergence concerning the idea of applying cyber sovereignty as a form of control over national territory. For example, the Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium, drafted in collaboration with the International Telecommunication Union, highlights the importance of access to information for the information society in paragraphs 24–28.

Since freedom of expression is not an unlimited fundamental right, restrictions are admissible if they are in accordance with the requirements of the limitation clause provided by paragraph 3 of Article 19. The 2011 General Comment No. 34 on freedom of expression of the Human Rights Council underlines this conclusion. Nevertheless, free access to the Internet and digital networks without any barriers, technical, structural or educational, is also supported by the OSCE.[66] Even the 2015 UNGGE Reports also expressly mention the need for the respect of fundamental rights, including the right to freedom of expression.[67] As a consequence, there must be a balance between the admissible actions of states and those that constitute interference with the normal exercise of this right and its content.[68] Establishing full state control over the infrastructure and flux of data and information as an effect of state cyber sovereignty would disproportionately and illegitimately impact the right to access information.

V Features of the Principle of State Sovereignty

In order to justify the idea of state sovereignty in cyberspace, the principle of territorial sovereignty is being used. However, there is no comprehensive definition of sovereignty in international law, so identifying its elements and meaning is highly relevant for the current analysis and for the legal consequences applicable in the traditional sense,

---

65 Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* Frank La Rue, 17th sess Agenda item 3 UN Doc A/HRC/17/27 (16 May 2011).

66 Organization for Security and Co-operation in Europe, The Representative on Freedom of the Media, Amsterdam Recommendations, Freedom of the Media and the Internet (14 June 2003), <https://www.osce.org/files/f/documents/4/a/41903.pdf > accessed 15 October 2024.

67 UN Doc A/70/174, § 13(e) Norm 5.

68 Gergely Gosztonyi, 'The European Court of Human Rights: Internet access as a means of receiving and imparting information and ideas' (2020) 6 (2) International Comparative Jurisprudence DOI: http://dx.doi.org/10.13165/j.icj.2020.12.003

some of the most important being state jurisdiction and state immunity,[69] which also constitute limits to other states' sovereignty. The complexity of the concept is amplified by the fact that the modern meaning of sovereignty refers to the peoples within a state, not exclusively to the state itself as a legal entity.[70] Sovereignty as a principle dates back to the 16th century[71] and is one of the concepts developed after the Peace of Westphalia of 1648. The Westphalian system considered States to have sovereignty over their territories and domestic affairs without the intervention of other States.

The principle of state sovereignty is one of the fundamental principles of international law, enshrined in Article 2, paragraph 1 of the Charter of the United Nations[72] and subsequent legal instruments (Declaration on principles of International Law friendly relations and cooperation among States in accordance with the Charter of the United Nations,[73] Helsinki Final Act,[74] Charter of Paris for a New Europe[75]) also mentioned this principle and its significant value for international law and established connections between it and other fundamental principles such as non-intervention, self-determination, territorial integrity and the peaceful solution of disputes.[76]

All interstate relations and the functioning of the state itself are based on this core principle. From a territorial perspective, state sovereignty and other fundamental principles of international law apply to all components of the territory of a state within its borders (terrestrial, maritime, airspace), where it enjoys undisputed exclusivity. All elements of state sovereignty refer to and are analysed in connection with physical state territory according to the stage of evolution of international law rules and concepts. Sovereignty describes the competencies of states and presents, in fact, multiple meanings.

---

69 Christopher Staker, 'Jurisdiction' in Malcolm D. Evans (ed), *International Law* (Oxford University Press 2014, Oxford) 309, DOI: https://doi.org/10.1093/he/9780198791836.003.0010

70 Samantha Besson, 'Sovereignty, International Law and Democracy' (2011) 22 (2) The European Journal of International Law 383, DOI: https://doi.org/10.1093/ejil/chr029

71 Andreas Osiander, 'Sovereignty, International Relations, and the Westphalian Myth' (2001) 55 (2) International Organization 251–287, DOI: https://doi.org/10.1162/00208180151140577

72 Article 2(1) of the Charter of the United Nations reads as follows: 'The Organization is based on the principle of the sovereign equality of all its Members'.

73 Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations (adopted 24 October 1970) 25th sess Supplement no 18 UNGA Res 2625 (XXV), A/RES/26/25 (XXV). The Declaration reads as follows on the principle of sovereignty: 'All States enjoy sovereign equality. They have equal rights and duties and are equal members of the international community, notwithstanding differences of an economic, social, political or other nature. In particular, sovereign equality.'

74 Conference on Security and Cooperation in Europe Final Act (adopted 1 August 1975) <https://www.osce.org/helsinki-final-act?download=true> accessed 15 October 2024.

75 Organization for Security and Co-operation in Europe, *Charter of Paris on a New Europe* (adopted 19-21 November 1990).

76 Helmut Steinberger, 'Sovereignty' in Rudolph Bernhardt (eds), *Encyclopedia of Public International Law* (Volume Four, Elsevier 2000, Amsterdam/New York/Oxford) 513.

Sovereignty is associated with the principle of equality, as enshrined in Article 2(1) of the Charter of the United Nations (sovereign equality), which underlines the independence[77] and the lack of subordination and power of one state over another. Sovereignty is the basic constitutional doctrine of the law of nations[78] seen as an essential and core attribute of the state both at the international and national level[79] and a premise for the existence of states and their international law personality. It is also an attribute of the state and an ideological concept without static or pre-established content,[80] which implies the possibility of different meanings from one period to another and the evolution of its features.

The contemporary meaning of sovereignty is territorial, as the state enjoys exclusive legal competence over its territory *(imperium)* and exercises ownership of real property *(dominium)*[81] within the borders of the state. In addressing the principle of sovereignty, many scholarly papers begin their legal analysis by referring to the conclusions of the *Island of Palmas Case*,[82] which analysed the territorial dimension of sovereignty as follows: 'Territorial sovereignty, as has already been said, involves the exclusive right to display the activities of a state. This right has as corollary a duty: the obligation to protect within the territory the rights of other states, in particular their right to integrity and inviolability in peace and in war, together with the rights which each State may claim for its nationals in foreign territory'.[83] At the same time, it must be stressed that the arbitration award considered the dynamic nature of the concept of sovereignty, as it stated: 'Manifestations of territorial sovereignty assume, it is true, different forms, according to conditions of time and place'.[84] This conclusion may be considered a means of the restrictive interpretation of state cyber sovereignty.

Sovereignty is based on the idea of a state exercising control or a display of authority in a given territory[85] or other space having special legal status. This includes authority and control over all individuals on the territory,[86] which implies exercising jurisdiction (prescriptive jurisdiction, jurisdiction to adjudicate, jurisdiction to enforce). Moreover, sovereignty means the power to freely dispose of the territory, the obligation for other states

---

77 Emmanuel Decaux, Olivier de Frouville, *Droit international public* (Dalloz 2016, Paris) 176.

78 Crawford (n 17) 447.

79 Jean Combacau, Serge Sur, *Droit international public* (12e edn, Librairie Générale de Droit et Jurisprudence 2016, Paris) 238.

80 Mohamed Bennouna, *Le droit international entre la lettre et l'esprit. Cours général de droit international public* (Tome 383, Brill /Nijhoff 2016, Leiden) 42.

81 Crawford (n 17) 204.

82 *Island of Palmas Case (or Miangas)* (United States of America v The Netherlands) (Award of the Tribunal) (Permanent Court of Arbitration, Arbitrator M. Huber, 4 April 1928) <https://pcacases.com/web/sendAttach/714> accessed 15 October 2024.

83 *Island of Palmas Case (or Miangas)* (United States of America v The Netherlands) 839.

84 *Island of Palmas Case (or Miangas)* (United States of America v The Netherlands) 840.

85 *Territorial and Maritime Dispute* (Nicaragua v Colombia) (Judgment) [2012] ICJ Rep 624.

86 Antonio Cassese, *International Law* (Oxford University Press 2005, Oxford) 49.

not to intrude on the state's territory *(jus excludendi alios),* the right to immunity from foreign courts and the right to immunity for state representatives.[87]

The meaning of the principle of sovereignty is the result of evolution, and it has a different significance than the one presented during the 16th and 17th centuries when it appeared as a result of European monarchies' intent to consolidate their position in relation to the church.[88] Therefore, there is an evolutive interpretation of the legal concept of sovereignty, according to which the meaning of sovereignty is subjective and different for states, taking into consideration their historical evolution.[89]

Applying the principle of sovereignty implies a correlative and reciprocal obligation to recognise other states as sovereign and to refrain from intervening in other state's affairs. On the other hand, sovereignty also implies the competences of the state and the exercise thereof from which derive jurisdiction and independence from other states.[90]

VI The Uncertainty of Cyber Sovereignty – Moving from *Iure Imperii* to *Iure Gestionis*?

1 Implications of Cyber Sovereignty

The term cyber sovereignty is used on quite a large scale at the moment. Yet its content and defining elements are unclear and vague.[91] According to the conclusion of UNGGE, a state enjoys sovereignty in relation to the ICT infrastructure on its territory,[92] but it cannot have sovereignty in the sense of control and exclusiveness over the data concerning private persons or private companies (such as personal data and data giving access to the banking digital system). If one transposes the sovereignty idea to the cyber environment, this implies exercising control therein over the elements that support sovereignty. In this regard, the works of GGE and OEWG do not refer to an abstract idea of sovereignty; they take into consideration the ICT infrastructure belonging to the state or located on its territory, which makes sense and is fully compatible with the features and elements of sovereignty. There is no clear position among states concerning the distinction between sovereignty as a principle and sovereignty as a rule.[93]

---

87 Cassese (n 86) 51–52.

88 Bennouna (n 80) 41.

89 Bennouna (n 80) 42.

90 Crawford (n 17) 448.

91 Baezner, Robin (n 10) 2.

92 von Heinegg (n 16) 19.

93 For further details and analysis, Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views,' (2020) The Hague Program for Cyber Norms Policy Brief 4–7. <https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views> accessed 15 October 2024.

On the other hand, the concept of cyber sovereignty is opposed to the idea of a completely free cyber environment accessible to all. It involves the potential of states to control the flow of data and information and to take control of these.[94]

The most important legal effect of recognising cyber sovereignty as implying an international obligation is that, in case of violation, the mechanism of international responsibility will be activated. In this regard, the award associated with the *Nicaragua* case by the International Court of Justice is relevant, which states the following: 'If a State acts in a way *prima facie* incompatible with a recognized rule, but defends its conduct by appealing to exceptions or justifications contained within the rule itself, then whether or not the State's conduct is in fact justifiable on that basis, the significance of that attitude is to confirm rather than to weaken the rule.'[95]

At the same time, we must observe the 'paradox' of sovereignty[96] concerning the connection between the existence of states and international law in this particular environment. In other words, the silence of states or their ambiguous position may be the best way to ensure the application of international law in cyberspace. On the other hand, cyber sovereignty may not refer exclusively to state governance,[97] taking into account the diversity of users and actors in cyberspace.

2 Cyber Sovereignty as a Form of Control

States consider the currently identified rules and principles for their conduct in cyberspace as a putative normative order[98] and the present digital empire should reconcile different types of approaches. State practice will be an essential element in clarifying aspects of sovereignty in cyberspace, as well as its scope and limits. However, states are reluctant to expressly present their position in this regard. Few states have adopted specific regulations in this area apart from declarations of principle expressed within the UN or other bodies, and their views have been publicly expressed.

The concept of cyber sovereignty was first used and intensely promoted by China and includes several prerogatives of the state, under national law, to regulate the conduct of private persons related to the Internet and the use of personal data within its territory as a means of protecting the information space, in accordance with the general policy on

94 Metcalf (n 12) 1.

95 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14, 98 [186].

96 'Is that states must be capable of binding themselves if International Law is to exist, and also incapable of binding themselves through International Law if they are to be absolutely independent.' Besson (n 70) 377.

97 Andrea Leiter, 'Cyber Sovereignty: A Snapshot from a field in motion' (2020) 61 Harvard International Law Journal Frontiers 2.

98 Nicholas Tsagourias, 'The Slow Process of Normativizing Cyberspace' (2019) 113 (71) American Journal of International Law Unbound 73, DOI: https://doi.org/10.1017/aju.2019.9

controlling the Internet and the flux of data.[99] The Golden Shield and Great Firewall of China started as a project in 1996 and was implemented in 2008. It is the perfect example in this regard, as it establishes full state control of information and access to information. It is a comprehensive system of Internet surveillance and censorship implemented by the government of China with the purpose of regulating online content and controlling the flow of information within its borders.[100] Scholars and ONGs have extensively documented the impact of the Golden Shield on freedom of expression and privacy in China. The analysis provides details of the legal and technical mechanisms used to implement Internet censorship and surveillance.[101]

Despite all censorship policies and measures adopted by China, it is building digital infrastructure in many countries around the world[102] together with the surveillance techniques that are acceptable to authoritarian countries. This approach is reflected and extended by the domestic legislation of the Russian Federation, which adopted in 2019 the *'Sovereign Internet Law'*,[103] establishing the legal framework for controlling the Internet inside its borders.[104] The Russian Federation claims that it has created its own national network, tests have already been undertaken, and users have not experienced any trouble or did not even realise the change. Previously, in December 2016, the President of the Russian Federation approved by Decree the Doctrine of Information Security.[105] This means creating its own national Internet and cyber environment and separating it from international cyberspace.[106] The Russian government employs various mechanisms to filter and censor online content, including the use of Internet filtering technology, blocking

---

[99] Broeders, Adamson, Creemers (n 15) 2.

[100] Gergely Gosztonyi, *Censorship from Plato to Social Media* (Springer 2023, Cham) 103–107, DOI: https://doi.org/10.1007/978-3-031-46529-1_7

[101] Maya Wang, 'China's Dystopian Push to Revolutionize Surveillance', (2017) <https://www.hrw.org/news/2017/08/18/chinas-dystopian-push-revolutionize-surveillance> 15 October 2024; Amnesty International, 'Freedom from Censorship! China's Choice, (2008) <https://www.amnesty.org/en/wp-content/uploads/2021/06/asa170322008eng.pdf> accessed 15 October 2024; Jonathon Keats, ''Great firewall', Virtual Words: Language on the Edge of Science and Technology' (Oxford University Press 2010, New York).

[102] Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press, New York, 2023), DOI: https://doi.org/10.1093/oso/9780197649268.001.0001

[103] Moynihan (n 7).

[104] Alena Epifanova, 'Deciphering Russia's "Sovereign Internet Law" Tightening Control and Accelerating the Splinternet' (2020) 2 German Council on Foreign Relations DGAP Analysis.

[105] It stated that 'The Constitution of the Russian Federation, universally recognized principles and norms of international law, international treaties signed by the Russian Federation... form the legal framework of the Doctrine' (§ 4) and that 'Information security activities of government bodies is based on the following principles... (e) compliance with the universally recognized principles and norms of international law, international treaties to which the Russian Federation is a party and laws of the Russian Federation' (§ 34) <http://www.scrf.gov.ru/security/information/DIB_engl/> accessed 15 October 2024.

[106] Elena Sherstoboeva, 'Russian Bans on 'Fake News' about the war in Ukraine: Conditional truth and unconditional loyalty' (2024) 86 (1) International Communication Gazette 36–54, DOI: https://doi.org/10.1177/17480485231220141

access to websites and social media platforms, and imposing restrictions on certain types of online content, such as political dissent or criticism of the government. Russia conducts extensive surveillance of Internet activities, including monitoring online communications, tracking individuals' browsing histories and intercepting electronic communications. This surveillance apparatus is used to identify and suppress dissenting voices, monitor political activists and opposition groups and maintain social control.[107]

The justification given by the Russian President is that these are security measures intended to protect the state in the event of an 'emergency or foreign threat like a cyberattack'.[108] Under the law, the state has the prerogative to control the Internet through Russian-controlled infrastructure and to create a system of domain names. From the perspective of its consequences, such a measure constitutes a disconnection of the Russian infrastructure network from the global network and constitutes censorship for its users.[109]

Such a technical possibility may be put into practice without great difficulty and could be seen as a display of territorial jurisdiction.[110] Yet, if all states created and isolated their national networks in the name of cyber sovereignty, the result would no longer correspond to the idea of an international global network as we know and use it today and would definitely involve sacrificing the Internet.[111] It would involve just an extension of the national territory, entirely controlled by the state, including control over data, the flux of data, users, technical parameters and the overall characteristics of this space.

A different approach, more tempered in this regard, is associated with France and was expressed in its 2017 International Strategy[112] and the 2018 Strategic Review of Cyberdefense.[113] The latter states that 'the principle of sovereignty applies to cyberspace. In this respect, France reaffirms its sovereignty over information and communication technologies (ICT) infrastructure [*systèmes d'information*], persons and cyber activities located within its territory, subject to its international legal obligations.'

In defining the threshold of a sovereignty breach, the approach focuses on the conduct representing the ICT system penetration, not the consequences. France has developed

---

[107] Gergely Gosztonyi, 'Special models of internet and content regulation in China and Russia' (2021) (2) ELTE Law Journal 87–99, DOI: https://doi.org/10.54148/ELTELJ.2021.2.87

[108] <https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html> accessed 15 October 2024.

[109] Gergely Ferenc Lendvai, 'Media in War: An Overview of the European Restrictions on Russian Media' (2023) 8 (3) European Papers 1235–1245, DOI: http://doi.org/10.15166/2499-8249/715

[110] von Heinegg (n 16) 9.

[111] Mueller (n 5) 5.

[112] 'La stratégie internationale de la France pour le numérique' 15 December 2017, France Diplomatie, <https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-strategie-internationale-de-la-france-pour-le-numerique> accessed 15 October 2024.

[113] François Delerue, Aude Géry, 'France's Cyberdefense Strategic Review and International Law' (2018) Lawfare <https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law> accessed 15 October 2024.

a national system of defining and qualifying the actions that constitute a cyber security incident.

Another example of a global approach to cyberspace was the National Cyber Strategy[114] of the United States of America. This focused on an open and global cyberspace and promoted 'a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime, and the consideration of practical confidence building measures to reduce the risk of conflict stemming from malicious cyber activity.[115] These principles should form a basis for cooperative responses to counter irresponsible state actions inconsistent with this framework.'

The new Strategy issued in 2023 focuses on resilience in cyberspace and highlights the threats presented by authoritarian governments such as China and North Korea.[116] The publicly expressed positions of states concerning sovereignty in cyberspace may be very different in practice, which makes it difficult to argue for the existence of an *opinio iuris* on how it applies, yet this does not infer a normative gap.[117] Australia expressed this position at the OEWG session on 2 July 2020, affirming the need to find topics of confluence between states in order to ensure a peaceful and stable cyberspace.[118]

The United Kingdom has also developed a national cybersecurity strategy, created a National Cyber Security Centre[119] and sustains the applicability of sovereignty as a principle, considering that there is no rule of sovereignty in cyberspace.[120] From a theoretical and practical perspective, the differences between the two approaches to sovereignty – as a principle and as a rule – are not very clear, and their effectiveness may not be significant because states have international obligations in each case.

---

[114] 'The White House, 'National Cyber Strategy of the United States of America' (2018) 20, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> accessed 15 October 2024.

[115] cf Roland Kelemen, Ádám Farkas, 'The relationship between social media platforms and hybrid conflicts' (2022) 11 (1) In Medias Res 96–108.

[116] The White House, 'National Cybersecurity Strategy' (2023) <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf> accessed 15 October 2024.

[117] Tolppa (n 32).

[118] *Australian Intervention*, OEWG Virtual Meeting: 2 July 2020, <https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-australia-2-july-2020.pdf> accessed 15 October 2024.

[119] See National Cyber Security Centre <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do> accessed 15 October 2024.

[120] Jeremy Wright, 'Cyber and International Law in the 21st Century' (2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 15 October 2024.

VII Conclusions

Additional efforts by states and international organisations are required to clarify the idea of cyber sovereignty by outlining its dimensions and restrictions in relation to the fundamental principle of state sovereignty. States asserting cyber sovereignty may impose restrictions on online content deemed to be offensive, harmful or contrary to national interests. While states have a legitimate interest in regulating certain types of content, such as hate speech or incitement to violence, overly broad or vague regulations can result in censorship and limit individuals' ability to exercise freedom of expression online.

In cyberspace, the interests of many parties are interconnected. The concept of cyber sovereignty contradicts the idea of global cyberspace governance and ignores the interests of other actors, such as private companies and individuals, who use cyberspace. There are no legal hurdles in international law to the regulation of cyberspace and the behaviour of states and other stakeholders. Actions may involve leveraging existing principles and standards that can be tailored to this unique environment. State sovereignty in cyberspace is limited and distinct from authority over physical territories. A pragmatic approach comprises understanding that state sovereignty in cyberspace pertains to the physical infrastructure underpinning cyberspace's existence while explaining concerns related to state jurisdiction, extraterritorial impacts and defining violations of sovereignty in cyberspace.

Adelina-Maria Tudurachi*

Internet Access as a Basic Human Right: An Ongoing European Legal Debate?

Abstract

The pervasive use of Information and Communication Technology has inevitably interfered with human rights worldwide. This persistent interaction has led to questioning the legal nature of Internet access itself: is it an autonomous right or an implicit right? This paper examines the relevant case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) in order to assess whether Internet access is today a basic human right. The Strasbourg jurisprudence stems mainly from applications based on freedom of expression and the right to education. The ECtHR applies the binary axiological test: the right for which protection is sought and the competing interest/right provided by the European Convention on Human Rights. So far, it has not explicitly recognised the right to Internet access but rather the Internet's widespread usage and importance. The Luxembourg case law constitutes proof of the economic dimension of the Union since the CJEU applies a threefold test, depending on the piece of legislation basing the application, and takes a moderate approach to questions involving human rights. Thus, the complementarity of ECtHR and CJEU case law proves that Internet access rather facilitates the exercise of other rights than is an autonomous right. For this reason, limitations are assessed on a case-by-case basis according to the requirements associated with each conventional right's specific restrictions.

Keywords: Internet access; fundamental rights; threefold conflict of values; freedom of expression; freedom to conduct business; copyright-related rights

* Dr Adelina-Maria Tudurachi, LLM/Master's Degree within the Faculty of Law, University of Bucharest and the Faculté de Droit, Université Paris 1–Sorbonne. ORCID iD: 0009-0001-9455-827X.

I Introduction

Ubiquitous, evolving and 'merely' essential. These appear to be a few of the most conspicuous traits of the Internet[1] nowadays. What if suddenly your access to the Internet was restricted to a limited number of web pages or, even worse, banned entirely? Taking this dystopian scenario a step further, what if the restriction or the ban impinged on a whole community? For the European space of freedom, security and justice delineated by the borders of the European Union (EU), these hypotheses appear to pertain only to Orwell's or Huxley's writings, yet other parts of the world seem to perceive these challenges as possible and even real.[2]

Undoubtedly, the Internet has transformed into an omnipresent tool. Recent data from the International Telecommunication Union prove the increasing trend to online presence: in 2020, 3.7 billion people were offline worldwide, while in 2023, the connectivity rate rose, with only 2.6 billion people offline worldwide. Accordingly, perspectives about the Internet have polarised both around utopian – that is, technophilic – and dystopian points of view.[3] Embedded in our lifestyle and daily habits, this instrument has become increasingly popular with individuals of various ages and socio-economic backgrounds insofar as to be qualified as a specificity of this era of humankind. However, to what extent is this factual popularity reflected in the legal lens? In other words, should Internet access be taken for granted as a convenient facility of the present era? May the same conclusion be drawn regarding the legal articulation of the right to Internet access?

Indeed, the rapid development of information and communication technology alongside the widespread use of the Internet has correspondingly led to stronger expectations about connectivity at the social level. For this reason, numerous areas of our lives have been forged on digital frameworks and concepts such as 'e-learning', 'e-justice', 'e-administration' and 'e-governance' are increasingly familiar. Of course, this desire for societal innovation has led to a surge in the frequency of interactions with human rights. Whether what is at stake is access to justice or the right to education, the clash between technology and human rights has become so visible that new debates have emerged[4] concerning the possibility of reconsidering the well-established normative framework of human rights to include a stand-

---

1 My analysis revealed that the European Court for Human Rights uses Internet in its capitalised form while the Court of Justice of the European Union uses this term in the non-capitalised version. For consistency purposes, this paper will rely on the capitalised form.

2 For a comprehensive overview of Internet shutdowns around the world, see the 2022 Report of Access Now and the #KeepItOn coalition, 'Weapons of control, shield of impunity. Internet shutdowns in 2022' <https://www.accessnow.org/internet-shutdowns-2022/> accessed 15 October 2024.

3 Steven Hick, Edward F. Halpin, Eric Hoskins, *Human Rights and the Internet* (Macmillan Press Ltd 2000, London) 12–13, DOI: https://doi.org/10.1057/9780333977705

4 Hendrik Mildebrath, *Internet access as a fundamental right. Exploring aspects of connectivity* (European Parliamentary Research Service 2021) 7–12.

alone right to Internet access.[5] At the United Nations (UN) level, for instance, numerous recommendations have been formulated in the last almost two decades regarding Internet access[6] in relation to 'two major dimensions of Internet access: freedom of expression in cyberspace […] and physical access to the Internet'.[7] From the perspective of the Council of Europe (CoE), the Parliamentary Assembly affirmed in 2014 that 'public authorities have a duty to ensure the effective enjoyment of the right to freedom of expression online' and thus recommended 'that the Council of Europe member States ensure the right to Internet access' in accordance with a series of 12 principles, reinforcing the need for developing a universal definition of the right to Internet access.[8]

While Internet shutdowns represent a conspicuous threat to human rights, the EU space appears to be quite safe from this point of view.[9] However, from the standpoint of the CoE, the right to Internet access is recognised only in specific situations – namely, in the case of individuals deprived of liberty as a right derived from freedom of expression or the right to education, hence leaving no room for generalisations.[10] Similarly, at the EU level, the current normative framework does not enshrine an explicit right to Internet access.[11] In contrast, the number of Internet users in the EU significantly increased from 67% in 2010 to 92% in 2023.[12] This status quo reflects the notable benefits and drawbacks that fuel the debate concerning the 'emancipation' of a derived or stand-alone right to connectivity.[13] In this respect, some specialists question the potential legal grounds of this emergent right, even exploring its constitutional legal basis,[14] while others perceive

---

5 Başak Çalı, 'The Case for the Right to Meaningful Access to the Internet as a Human Right in International Law' in Andreas Von Arnauld, Kerstin Von Der Decken, Mart Susi (eds), *The Cambridge Handbook of New Human Rights* (Cambridge University Press 2020, Cambridge) 277–278. DOI: https://doi.org/10.1017/9781108676106

6 Łukasz Szoszkiewicz, 'Internet Access as a New Human Right? State of the Art on the Threshold of 2020' (2018) 8 Przegląd Prawniczy Uniwersytetu im Adama Mickiewicza 49–62, DOI: https://doi.org/10.14746/ppuam.2018.8.03. According to the author's quantitative analysis, between 2007 and 2017, the committees functioning under the United Nations umbrella mentioned the word 'Internet' in 246 recommendations.

7 Szoszkiewicz (n 6) 57.

8 Parliamentary Assembly of the Council of Europe, The right to Internet access, Resolution 1987 (2014) 9th April 2014.

9 According to the mid-year update provided by Access Now, the Internet shutdown phenomenon has persisted, and new reasons to disrupt Internet access during key national moments have been advanced, eg, catching fugitives in Mauritania or stopping protests in Pakistan: <https://www.accessnow.org/publication/internet-shutdowns-in-2023-mid-year-update/#join-us> accessed 15 October 2024.

10 Mildebrath (n 4) 29–30.

11 Article 36 of the CFR related to access to services of general economic interest might be a potential legal basis for this right. For details on this thesis, see Mildebrath (n 4) 32–34.

12 Eurostat, Digital economy and society statistics – households and individuals, <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access_of_individuals.2C_2010_and_2023> accessed 15 October 2024.

13 Mildebrath (n 4) 24–28.

14 Oreste Pollicino, 'The Right to Internet Access: Quid Iuris?' in Andreas Von Arnauld, Kerstin Von Der Decken, Mart Susi (eds), *The Cambridge Handbook of New Human Rights* (Cambridge University Press 2020, Cambridge) 271, DOI: https://doi.org/10.1017/9781108676106.021

it as an 'enabler' of other rights.[15] In accordance with this latter point of view, it has been argued that 'Internet access is not merely a luxury for those who can afford it but instead necessary for individuals to lead minimally decent lives'.[16] Contrastingly, some specialists deny its autonomous existence,[17] whereas other stakeholders advance the corresponding counterargument,[18] inflaming the legal discussion.[19]

Should this newly crafted right also imply a certain level of network security, a right to access digital literacy training services, the supply of a terminal device or even an independent right to access social media networks?[20] Some scholars argue that current UN-based soft law advocates 'the necessity of expanding Internet infrastructure, ensuring its affordability, and the importance of building digital literacy in […] society, particularly in the most disadvantaged and marginalised groups'.[21] Regardless of the potential answers, it is certain that 'the right to Internet access is a solid and much-needed guarantee for the democratic dimension of human lives, both in the bit and in the atomic dimensions', with due regard to 'net neutrality'.[22]

It goes without saying that the apparently underequipped legal framework may be enhanced in scope and mission by means of the judiciary. It appears as no surprise that 'the courts will play a critical role in shaping a legal framework, the boundaries of which are still flexible and indirectly call for (judicial) interpretation'.[23] In other words, the increasing role of the judiciary in transnational matters related to the relation between law and technology may be explained as follows: 'The burden of making up for this inevitable legislative inertia – at national and supranational level – falls heavily on the shoulders of the courts'.[24]

---

15 Nicola Lucchi, 'The Role of Internet Access in Enabling Individual's Rights and Freedoms' 2013/47 EUI Working Paper RSCAS 14. According to the author, the effervescence of the contemporary public debate around Internet access constitutes 'an essential element to give an updated meaning and application to already recognized fundamental legal rights'.

16 Merten Reglitz, 'The Human Right to Free Internet Access' (2020) 37 (2) Journal of Applied Philosophy 327, DOI: https://doi.org/10.1111/japp.12395

17 Vinton G. Cerf, 'Internet Access Is Not a Human Right' (4 January 2012) The New York Times, <https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=1&ref=opinion> accessed 15 October 2024.

18 Scott Edwards, 'Is Internet access a human right' <https://www.amnestyusa.org/updates/is-internet-access-a-human-right/> accessed 15 October 2024.

19 Media Defence, 'Is there a Right to the Internet under International Law?' <https://www.mediadefence.org/ereader/publications/introductory-modules-on-digital-rights-and-freedom-of-expression-online/module-3-access-to-the-internet/is-there-a-right-to-the-internet-under-international-law/> accessed 15 October 2024.

20 Mildebrath (n 4) 22.

21 Szoszkiewicz (n 6) 59.

22 Marco Bassini, Giovanni De Gregorio, Oreste Pollicino, *Internet Law and Protection of Fundamental Rights* (EGEA Spa – Bocconi University Press 2022, Milan) 49–50.

23 Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet A Road Towards Digital Constitutionalism* (Hart Publishing 2021, London) 197, DOI: https://doi.org/10.5040/9781509912728

24 Gergely Gosztonyi, *Censorship from Plato to Social Media. The Complexity of Social Media's Content Regulation and Moderation Practices* (Springer 2023, Cham) 12, DOI: https://doi.org/10.1007/978-3-031-46529-1_2

Bearing these observations in mind, the present paper aims to verify whether the EU actually provides its nationals with a truly safe area as regards Internet access, hence deepening the debate concerning the legal nature of Internet access as an autonomous human right or a means enabling the exercise of other rights.

First, this contribution outlines the European Court of Human Rights (ECtHR) case law regarding Internet access, especially the most recent developments regarding this matter. The analysis focuses on the current legal architecture of the European Convention of Human Rights (ECHR or Convention), which does not expressly secure the right to Internet access *per se*. Thus, the paper notes the subtle interference between Internet access and the exercise of other human rights, eg the well-known freedom of expression, as well as the right to education, in order to underline the recognition and the standard of protection developed by the Strasbourg Court.

Second, the analysis aims to emphasise the EU perspective on the matter through the lens of the relevant case law of the Court of Justice of the European Union (CJEU). Closely linked to the functioning of the single market, from the point of view of the Luxembourg Court, Internet access appears to have a prevalent economic dimension, hence being imbued with a rather faded human rights legal nature. It is the status of Internet access that the present contribution discusses, in accordance with the current legal framework. Correspondingly, the potential overlap between the perspectives of Strasbourg and Luxembourg is under scrutiny in light of the provisions of Article 52 of the Charter of Fundamental Rights of the European Union (CFR).

Last, the limitations of the right to Internet access are assessed. It goes without saying that the geo-political international context nowadays reveals a rather tense configuration of global affairs. This could trigger governments or individuals to resort to restrictive measures that could affect access to the Internet to a certain extent. Taking this into account, the paper discusses the scale of legitimacy that is applicable to Internet access limitations in light of the case law of the two European courts.

II The ECtHR Perspective – A Crossroads with Freedom of Expression and Right to Education

It is undisputed that the ECHR does not provide *expressis verbis* for a right to Internet access. Yet, the Strasbourg Court has ruled in some recent cases as regards the emergence of the aforementioned right. By means of these judgments, the ECtHR acknowledged the role of the Internet nowadays and implicitly underlined its potential judicial enshrinement in the conventional block of legal norms and protections. To begin with, on various occasions, the ECtHR was confronted with the legal qualification of the Internet. In fact, the timeline of the Strasbourg Court's attention to the increasingly impactful role of the Internet in the development of human rights is a few decades old since it initially ruled on this legal matter

in *Times Newspapers Ltd v the United Kingdom (nos. 1 and 2)* in March 2009: 'In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general'.[25]

The same perspective has already been developed in connection to freedom of expression, as safeguarded by means of service providers' liability, namely in *Delfi AS v Estonia*:

> The Court notes at the outset that user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression. That is undisputed and has been recognised by the Court on previous occasions […] However, alongside these benefits, certain dangers may also arise. Defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online.[26]

In the same context, the ECtHR acknowledged the role of the Internet while underlining the potential threats it brought about, that is, 'the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press'.[27]

This perspective has been maintained until the present time, as revealed by the recent judgement delivered in the case *Kilin v Russia*,[28] in which the Court admitted the omnipresence of the information and technology phenomenon:

> (...) The Court reiterates in this connection that owing to its accessibility and capacity to store and communicate vast amounts of information, the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information. The Internet provides essential tools for participation in activities and discussions concerning political issues and issues of general interest; it enhances the public's access to news and facilitates the dissemination of information in general. Article 10 of the Convention guarantees "everyone" the freedom to receive and impart information and ideas.

---

25 *Times Newspapers Ltd v the United Kingdom (nos. 1 and 2)*, no. 3002/03, 23676/03, § 27, 10 March 2009.

26 *Delfi AS v Estonia*, no. 64569/09, § 110, 16 June 2015. In this case, the applicant company complained that holding it liable for the comments posted by the readers of its Internet news portal infringed its freedom of expression as provided for in Article 10 of the Convention. The Court concluded there was no such violation.

27 *Delfi AS v Estonia*, § 133.

28 *Kilin v Russia*, no. 10271/12, § 54, 11 May 2021. The case concerned the applicant's criminal conviction for public calls to violence and ethnic discord on account of video and audio files that had been made accessible via a social network account. The Court found no violation of Article 10 related to freedom of expression.

> It applies not only to the content of information but also to the means of its dissemination, for any restriction imposed on the latter necessarily interferes with that freedom (…)

Bearing this in mind, the Strasbourg Court has dealt with several cases in which the factual situations assessed represented various configurations of the Internet's impact on human rights development. On the one hand, freedom of expression 'reached a turning point with the advent of the Internet, which was seen in its early days as a means of communication offering complete freedom',[29] thus generating several innovative judicial interpretations. On the other hand, the right to education interacted with the technological process at its own pace. Finally, ECtHR's case law offers an innovative view of the potential conflict between technology *lato sensu* and the respect due to contractual undertakings.

1 The Right to Receive and Impart Information – A Contemporary Perspective concerning those Deprived of Liberty

First, the situation of prisoners' access to the Internet seems to appear quite frequently before the Strasbourg Court, thus emphasising the values to be reconciled, namely the rights enshrined by the ECHR and the inherent restrictions imposed on prisoners.

With facts dating from 2005-2008, in *Kalda v Estonia*, the applicant was serving a lifetime imprisonment sentence, and the authorities refused to grant him access to a series of websites.[30] Namely, Pärnu Prison refused him access to the online version of the State Gazette, the decisions of the Supreme Court and administrative courts and the HUDOC database, whereas Tartu Prison, where he had been transferred, refused the applicant's request to be granted access to the Internet sites of the Council of Europe Information Office in Tallinn, the Chancellor of Justice and the Estonian Parliament. According to his allegations, the Estonian state was limiting prisoners' Internet access to the official databases of legislation and the database of judicial decisions. Therefore, these refusals hampered his judicial defence strategy in a number of legal disputes with the prison administration.[31]

The Strasbourg Court ruled that the Estonian state's conduct had infringed Article 10 of the ECHR. While the measure had been prescribed by law and pursued a legitimate aim, ie the protection of the rights of others and the prevention of disorder and crime, the necessity requirement had failed to be verified. The ECtHR took into account the informative content of the websites and the legal research purpose of their access:

---

[29] Gosztonyi (n 24) 169, DOI: https://doi.org/10.1007/978-3-031-46529-1_12

[30] *Kalda v Estonia*, no. 17429/10, 19 January 2016.

[31] Gergely Ferenc Lendvai, Gergely Gosztonyi, '"Access Denied" – Interpreting the Digital Divide by Examining the Right of Prisoners to Access the Internet in the Case Law of the European Court of Human Rights' (2024) 17 (1) Baltic Journal of Law & Politics 223–237, DOI: https://doi.org/10.2478/bjlp-2024-0011

> […] the websites to which the applicant wished to have access predominantly contained legal information and information related to fundamental rights, including the rights of prisoners. […] The Court considers that the accessibility of such information promotes public awareness and respect for human rights and gives weight to the applicant's argument that the Estonian courts used such information and the applicant needed access to it for the protection of his rights in the court proceedings.[32]

In addition, the Strasbourg Court took note of Estonia's elevated degree of digitisation insofar as the official publication of legal acts is done online. Furthermore, prisoners' general access to the Internet was equally assessed in the sense that national legislation provided for limited access to the Internet by means of computers specially adapted for that purpose and under the supervision of the prison authorities. In the absence of a concrete security risk assessment on the part of national authorities and given the lack of proof as regards additional costs, the ECtHR concluded that the interference was not sufficiently justified.[33]

It is worth noting that the ECtHR underlined the Internet's current societal role, as previously examined in *Delfi AS v Estonia*,[34] and further developed this perspective by stating that:

> The Court cannot overlook the fact that in a number of Council of Europe and other international instruments, the public-service value of the Internet and its importance for the enjoyment of a range of human rights has been recognised. Internet access has increasingly been understood as a right, and calls have been made to develop effective policies to attain universal access to the Internet and to overcome the "digital divide" (…) The Court considers that these developments reflect the important role the Internet plays in people's everyday lives. Indeed, an increasing amount of services and information is only available on the Internet […].[35]

In a comparable fashion, the case of *Jankovskis v Lithuania* underscores the link between the Internet and freedom of expression in its component referring to receiving and imparting information and ideas.[36] In the latter case, with facts dating from 2006-2007, the applicant was serving an imprisonment sentence and complained that he did not have Internet access in prison, more specifically to a state-administered website which contained information about learning and study programmes in Lithuania. Hence, he was prevented from receiving education-related information concerning the possibility of enrolling at a university in order to continue his higher education (to acquire a second university degree) in a distance-learning format.

---

32 *Kalda v Estonia*, § 50.
33 *Kalda v Estonia*, § 53.
34 *Kalda v Estonia*, § 44.
35 *Kalda v Estonia*, § 52.
36 *Jankovskis v Lithuania*, no. 21575/08, 17 January 2017.

The Court concluded that Article 10 of the ECHR had been infringed. In applying its three-step test,[37] the ECtHR acknowledged there had been an interference with the applicant's right, which was prescribed by national law and pursued the legitimate aim of protecting the rights of others and preventing disorder and crime. Still, when assessing the necessity of the measure, ie the Internet ban applicable to prisoners, the Strasbourg Court concluded that this condition was not fulfilled. In this respect, the ECtHR paid attention to the relevance of such information to the applicant's educational perspective, rehabilitation and reintegration into society. Added to this, the Court observed the efficiency of web browsing study programmes, the lack of other adequate education alternatives in prison, and the reticence of state authorities to grant at least limited or controlled access to the Internet.[38]

Notably, this case reinforces the Strasbourg view already developed in *Kalda v Estonia* regarding the Internet's role concerning human rights, more specifically, freedom of expression. As already noted by legal specialists, in this case, the Strasbourg Court made only some particular observations in slightly different terms, which may not be interpreted in a general manner, hence remaining rather cautious.[39] Still, it appears quite surprising that, in spite of the targeted online content, the legal grounds of the complaint did not make any reference to the right to education:

> […] the Court is mindful of the fact that in a number of the Council of Europe's and other international instruments[,] the public-service value of the Internet and its importance for the enjoyment of a range of human rights has been recognised. Internet access has increasingly been understood as a right, and calls have been made to develop effective policies to achieve universal access to the Internet and to overcome the "digital divide" (…) The Court considers that these developments reflect the important role the Internet plays in people's everyday lives, in particular since certain information is exclusively available on [the] Internet.[40]

A similar approach may be identified in the case *Ramazan Demir v Turkey*, which represented an adequate occasion for the ECtHR to rule on similar matters beyond the EU space and in matters dating from 2016, thus obviously more recent.[41] In this case, the applicant was a lawyer subject to a preventative measure who requested permission from the prison authorities to access the Internet sites of the ECtHR, the Constitutional Court and

---

37 William A. Schabas, *The European Convention on Human Rights: A Commentary* (Oxford University Press 2015, New York) 468–480.

38 *Jankovskis v Lithuania*, § 59–62.

39 Lina Jasmontaite, Paul de Hert, 'Access To The Internet In The EU: A Policy Priority, A Fundamental, A Human Right Or A Concern For Egovernment?' (6) 2020/19 Brussels Privacy Hub Working Paper 13. DOI: https://doi.org/10.2139/ssrn.3535718

40 *Jankovskis v Lithuania*, § 62.

41 *Ramazan Demir v Turkey*, no. 68550/17, 9 February 2021.

the Official Gazette, arguing that these information sources were necessary for preparing his own defence and following his client's cases. While national law provided for prisoners' access to the Internet, subject to supervision by the prison authorities and in view of training and rehabilitation programmes, his request was rejected by the authorities.

The Strasbourg Court ruled that Article 10 had been violated in this case. Consistent with its previous case law, namely *Kalda* and *Jankovskis*, the ECtHR admitted that the impugned restriction constituted an interference with the applicant's right to receive and impart ideas, which was prescribed by law yet not necessary in a democratic society. In this respect, the legal debate focused on the assessment and reasoning of national judicial authorities. As the Court observed, the domestic court did not examine in an adequate and detailed manner the security risks triggered by the applicant's access to the three websites, especially since these belonged to state authorities or to an international organisation, and his access took place under authorities' control and in accordance with the conditions therein determined.[42] This analysis shall be complemented by the case law developed under Article 2 of Protocol No. 2 of the ECHR.

2 Educational Needs in Prison – A Legal Bedrock for an Emerging Right to Internet Access

From a different perspective, the case *Mehmet Reşit Arslan and Orhan Bingöl v Turkey* stands out due to its focus on the right to education.[43] The two applicants, who were serving life imprisonment sentences, complained about restrictions imposed on their use of a computer and access to the Internet, which facilities they considered vital for pursuing higher education and developing their general knowledge. The first applicant had been a student at the faculty of medicine, and his request to access a computer and Internet was refused by prison authorities; yet, afterwards, he enrolled in the faculty of economics and management, which provided distance learning courses. Concerning the latter, for security reasons, the national authorities drastically restricted his use of an electronic device equipped with computing and English-Turkish translation functions to once per fortnight, for only one hour, in the library. The other applicant was admitted to higher education in the field of computer programming in a distance learning format, which required access to a computer and the Internet, but his request for the latter was rejected by the prison authorities. As regards the timeframe, it must be highlighted that the facts date from 2006-2007.

Sua sponte, the Strasbourg Court examined their complaints from the point of view of Article 2 of Protocol No. 2 of the Convention and found a violation thereof regarding both applicants. The Court applied the three-step test, which is defined in this case as a

[42] *Ramazan Demir v Turkey*, § 46.

[43] *Mehmet Reşit Arslan and Orhan Bingöl v Turkey*, no. 47121/06, 13988/07, 34750/07, 18 June 2019.

non-exhaustive list of legitimate aims. Expectedly, given the similarity of factual situations, it took 'due account of its case law, hitherto developed under Article 10 of the ECHR, on the right of prisoners to Internet access', more specifically, *Kalda* and *Jankovskis*. Thus, the scrutiny of the ECtHR could be summarised as follows: 'In order to determine whether a refusal to provide prisoners with Internet access is justified in a given case, an assessment should be made of whether the domestic courts conducted an adequate evaluation of the actual risks to security inherent in the particular case, thus properly balancing the competing interests.'[44]

It is noteworthy that, in this case, the role of the Internet appears rather ancillary and less significant. Indeed, according to the facts of the case, the prisoners were allowed to use a computer and have access to the Internet in the premises designated for that purpose by the prison authorities in the framework of rehabilitation and training programmes, and Internet use could be monitored by the authorities to the extent required by the relevant training and rehabilitation programmes. Far from being granted the status of a severable or autonomous right, in this case, Internet use was understood solely to constitute a means of exercising the right to education; thus, the legal question appears to be the reasoning process of the national judicial authorities:

> In the Court's view, there can be no doubt that the manner and means of regulating the mode of access to such facilities in prison fall within the Contracting State's margin of appreciation. It is enough for the Court to seek to ascertain whether the domestic courts, on the one hand, carried out the requisite balancing of the various competing interests in the present case, and on the other fulfilled their obligation to prevent any abuse on the authorities' part in implementing the relevant domestic rules.[45]

The sphere of human rights impacted by information and communication technology is not confined only to freedom of expression and the right to education. Thus, the aforementioned interaction has unexpected legal implications.

3 Are Electronic Means of Communication more Important than Contractual Obligations?

Finally, it is surprising that the ECtHR's mission of safeguarding human rights, specifically freedom of expression, may even interfere with apparently private disputes, as is the case in *Khurshid Mustafa and Tarzibachi v Sweden*.[46] In this case, the applicants concluded a rental agreement for a flat in Stockholm, which stated that the 'tenants were obliged to take proper care of the flat and to maintain good sanitary conditions, order, and good

[44] *Mehmet Reşit Arslan and Orhan Bingöl v Turkey*, § 59.
[45] *Mehmet Reşit Arslan and Orhan Bingöl v Turkey*, § 64.
[46] *Khurshid Mustafa and Tarzibachi v Sweden*, no. 23883/06, 16 December 2008.

practice in the house'. When moving in, a satellite dish was mounted on the façade of the building, next to one of the windows of the flat, which the applicants used in order to receive television programmes in Arabic and Farsi. After their landlord changed, they were required to dismantle the dish mainly for safety reasons in the case of a break in the tenancy contract. Failing to comply, they were served with a notice terminating the tenancy, and despite having replaced the satellite dish with a mobile unit, the landlord started proceedings, which concluded with the applicants' eviction from the flat, even though the only concern of the landlord was aesthetic dissatisfaction.

On the one hand, as regards admissibility, this judgement concerned the intervention of the ECtHR in contractual matters. In fact, the state's responsibility could be engaged since it stemmed from the effects of a national court's ruling. In this respect,

> […] the Court is not in theory required to settle disputes of a purely private nature. That being said, in exercising the European supervision incumbent on it, it cannot remain passive where a national court's interpretation of a legal act, be it a testamentary disposition, a private contract, a public document, a statutory provision or an administrative practice appears unreasonable, arbitrary, discriminatory or, more broadly, inconsistent with the principles underlying the Convention.[47]

On the other hand, as regards the merits, the ECtHR found a violation of Article 10 of the ECHR. The reasoning of the Court relied on the concrete usefulness of the television programmes accessed via the satellite dish:

> […] the Court observes that the applicants wished to receive television programmes in Arabic and Farsi from their native country or region. That information included, for instance, political and social news that could be of particular interest to the applicants as immigrants from Iraq. Moreover, while such news might be the most important information protected by Article 10, the freedom to receive information does not extend only to reports of events of public concern, but covers in principle also cultural expressions as well as pure entertainment. The importance of the latter types of information should not be underestimated, especially for an immigrant family with three children, who may wish to maintain contact with the culture and language of their country of origin. The right at issue was therefore of particular importance to the applicants.[48]

At the same time, the Court took into consideration the scarcity of the means to acquire information in their native language:

[47] *Khurshid Mustafa and Tarzibachi v Sweden*, § 33.
[48] *Khurshid Mustafa and Tarzibachi v Sweden,* § 44.

> […] it has not been claimed that the applicants had any other means of receiving these or similar programmes at the time of the impugned decision than through the use of the satellite installation in question, nor that their satellite dish could be installed in a different location. They might have been able to obtain some news through foreign newspapers and radio programmes, but these sources of information only cover parts of what is available via television broadcasts and cannot in any way be equated with the latter. Moreover, it has not been shown that the landlord later installed broadband and internet access or other alternative means which gave the tenants in the building the possibility to receive these television programmes.[49]

It is this latter argument that is of utmost importance to our analysis. In other words, the applicants' right to receive and impart information in their native language was deemed much more significant in the context of the shortage of electronic communication methods for maintaining a connection with the cultural and linguistic heritage of their country of origin. It is for this specific reason that, *mutatis mutandis*, Internet access could be deemed as overriding the contractual interests of others. Although this interpretation might be deemed as going further than the Court's intention, it seems reasonable to adopt this stance given the technological evolutions that have occurred since the time of the facts (1999-2004).

From this closer scrutiny of case law, it seems that the ECtHR is fully aware of the growing importance of the Internet and its impactful interference with human rights. While a stand-alone right has not been so far recognised, not even by applying the evolutive method of interpretation, access to the Internet has interfered with several Convention-safeguarded rights and freedoms.[50] Among them, freedom of expression appears to be the most conspicuous bedrock for assessing the Internet's impact as regards receiving and imparting information, yet the ECtHR's findings may not be generalised. Only the content-based analysis of such information may give rise to a different legal basis, namely, the right to education. All in all, the Court chose a rather cautious approach without actually embracing a clear position as to the severability of this right. It seems that in the absence of a legal instrument positively enshrining this right, the legal debate at the CoE level remains in the soft law sphere.

---

[49] *Khurshid Mustafa and Tarzibachi v Sweden,* § 45.

[50] Adam Wiśniewski, 'The European Court of Human Rights and Internet-Related Cases' (2021) 26 (3) Białostockie Studia Prawnicze 109–133, DOI: https://doi.org/10.15290/bsp.2021.26.03.06. According to the author, such Internet-related cases represent proof of Strasbourg Court's capacity to dynamically develop the 20th-century conventional provisions, hence shaping updated standards as regards human rights protection.

III The Luxembourg Point of View – An Enhanced Threefold Conflict

It goes without saying that the debate revolving around the right to Internet access is also noticeable at the EU level. In this respect, the human rights legal framework does not explicitly recognise such a right. However, legal specialists argue that the current normative architecture allows for the respect of such a right by virtue of Article 36 CFR.[51] In light of its scope and role, the Charter itself gives enough leeway for successfully enshrining such a right, subject to the limitations imposed by Article 51 CFR, namely the interlink between the specific right and EU law application.[52] In this respect, the latest developments underscore three potential scenarios: the policies and actions of Member States in view of incorporating the right to Internet access, the innovative interpretation method applied by the Luxembourg and Strasbourg courts, or formal recognition as a result of international developments.[53]

Bearing these hypotheses in mind, the CJUE's point of view may be most effectively assessed by means of its recent case law. Thus, in its 2019 case *Google (Territorial scope of de-referencing)*, the Luxembourg Court was called to decide on the 'balance between the right to privacy and the protection of personal data, on the one hand, and the freedom of information of internet users, on the other [which] is likely to vary significantly around the world.'[54] Similarly, a bipartite clash of rights was assessed in the case of *Tommy Hilfiger Licensing and others*, which emphasised the fair balance which must be struck between 'the protection of intellectual property and the absence of obstacles to legitimate trade'.[55]

Still, the human rights debate is particularly obvious when immixtures with various CFR-safeguarded rights are analysed. This is the case of national injunctions on various grounds and legal instruments that give rise to the fruitful development of the human rights framework. As such, both the *UPC Telekabel Wien* case and the *Mc Fadden* case underline the threefold axiological conflict between copyright-related rights, freedom to conduct business and freedom of expression.

---

51 Mildebrath (n 4) 32–33. For an overview of the scope of this right, see Paul Craig, Gráinne de Búrca, *EU Law. Text, Cases, and Materials* (Oxford University Press 2011, New York) 1073–1074.

52 Mildebrath (n 4) 33.

53 Jasmontaite, de Hert (n 39) 11–13.

54 Case C-507/17 *Google LLC, successor to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL),* EU:C:2019:772, § 60.

55 Case C-494/15 *Tommy Hilfiger Licensing LLC, Urban Trends Trading BV, Rado Uhren AG, Facton Kft., Lacoste SA, Burberry Ltd v Delta Center a.s.*, EU:C:2016:528, para 35.

1 The UPC Telekabel Wien Case[56] – The Cinematographic Injunction

Delivered on 27 March 2014, the abovementioned case stirred the interest of scholars from various points of view, such as the liability of service providers.[57] However, the present analysis focuses solely on the human rights assessment.

The facts of the case may be briefly summarised as follows: Constantin Film and Wega discovered that a website was offering, without their consent, either a download or 'streaming' of some of the films they had produced in violation of their copyright-related rights. The two film production companies applied for interim measures to obtain an order obliging UPC Telekabel, an Internet service provider, to block the access of its customers to the website at issue.

Procedurally speaking, the court of first instance, *Handelsgericht Wien* (Commercial Court, Vienna), prohibited UPC Telekabel from providing its customers with access to the website at issue, which led to the blocking of the site's domain name and current IP address and any other IP addresses of that site. Then, the higher court, *Oberlandesgericht Wien* (Higher Regional Court), partially reversed the order, establishing that UPC Telekabel could only be required, in the form of an obligation to achieve a particular result, to forbid its customers access to the website at issue, but that it must remain free to decide the means to be used. Finally, the highest court, *Oberster Gerichtshof* (Supreme Court), stayed the proceedings in view of the preliminary ruling request at stake.

Before analysing the judgment, it is worth paying attention to the Opinion of Advocate General Cruz Villalón, which is notable for at least two reasons.[58] On the one hand, the threefold conflict of values is underscored, namely, the balance that must be struck between the rights safeguarded by means of the specific EU instrument, ie copyright, and the other concurring rights.[59] In this case, alongside copyright protection as enshrined by Article 8(3) of Directive 2001/29/EC, the Advocate General (AG) observed the impact on freedom of expression, protected by Article 11 CFR, as well as on freedom to conduct business, safeguarded by Article 16 CFR. Regarding freedom of expression, the AG highlighted that 'the blocking measure does actually affect infringing material and that there is no danger of blocking access to lawful material.'[60] On the other hand, the opinion of the AG proves to be coherent with the Strasbourg perspective since the case law of the ECtHR is taken into account. In this respect, the AG underlined that 'the access to information afforded by the Internet is today considered essential in a democratic society',[61] having regard to the

---

[56] Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, EU:C:2014:192.

[57] Gosztonyi (n 24) 134–135, DOI: https://doi.org/10.1007/978-3-031-46529-1_9

[58] Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, Opinion of AG Cruz Villalón, EU:C:2013:781.

[59] *UPC Telekabel Wien*, Opinion of AG Cruz Villalón, § 81.

[60] *UPC Telekabel Wien*, Opinion of AG Cruz Villalón, § 82.

[61] *UPC Telekabel Wien*, Opinion of AG Cruz Villalón, § 108.

praetorian developments stemming from the 2012 case *Yildirim v Turkey*, including the comparative law survey led by the Council of Europe survey on this matter.[62] Bearing these observations in mind, the AG took the view that prohibiting an internet service provider 'in quite general terms and without ordering specific measures, from allowing its customers access to a particular copyright-infringing website' is not compatible with the balance test of fundamental rights.

The judgment of the Luxembourg Court is remarkable from two points of view. Not only does it acknowledge the threefold conflict of values emphasised by the AG in his Opinion,[63] but it also highlights the interference with Internet users' rights.[64] In this respect, the Court outlined the strict requirements that must be met by injunctions associated with the online ecosystem:

> […] the measures adopted by the internet service provider must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services in order to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued.[65]

For these reasons, the CJEU embraced a different perspective from the AG and allowed for such a prohibition subject to certain conditions. First, the compatibility depends on whether respect for Internet users' freedom of expression is respected.[66] Second, such prohibitions must equally safeguard copyright-related rights.[67]

To conclude, in *UPC Telekabel Wien*, the Court adopted no explicit stance as to the potential autonomy of the right to Internet access. In fact, it rather chose the EU-specific moderate approach that connects Internet access to freedom of expression and its component, access to receive and impart information. Refraining from any reference to the Strasbourg point of view, the CJEU undertook close scrutiny of the human rights at stake and, surprisingly or not, decided to award particular importance to online freedom of expression without qualifying it as a stand-alone right.

---

62 *Ahmet Yildirim v Turkey*, no. 3111/10, 18 December 2012, § 31. According to this survey, 20 Member States protect this right constitutionally by means of the guarantees granted to freedom of expression.

63 *UPC Telekabel Wien*, § 47.

64 *UPC Telekabel Wien*, § 55.

65 *UPC Telekabel Wien*, § 56.

66 In its operative part, the CJEU established that 'the measures taken do not unnecessarily deprive internet users of the possibility of lawfully accessing the information available'.

67 The CJEU stated that the measures taken must 'have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right, that being a matter for the national authorities and courts to establish.'

2 The Mc Fadden Analysis – The Insecure Internet Network

While the *Spiegel Online* case focused on the conflict between copyright-related rights (namely the author's exclusive rights or reproduction and communication to the public, on the one hand, and the fundamental rights of users of that specific intellectual work, in particular, their freedom of expression and information), the judicial analysis provided a valuable view of this latter right, yet, overall, an incomplete one.[68] The same bipartite exercise of weighing the interests at stake may be identified in *Funke Medien NRW* with regard to refused access to confidential documents,[69] as well as in *Pelham and Others*, which concerned the copyright protection of a phonogram, more specifically, the alleged copying of approximately two seconds of a rhythmic sequence.[70] What all these cases have in common is the fact that private rights, namely copyright-related ones, are weighed against freedom of expression. While this exercise is noteworthy in itself, it seems quite common in relation to the developments in the ECtHR.

A more comprehensive legal analysis may be observed in *Mc Fadden*,[71] which involved a distinct tripartite balancing test. This time, though, the interests at stake seem to be more deeply imbued with the EU's specificities since freedom of expression is opposed both with copyright-related rights and freedom to conduct business. Still, the EU instrument in discussion is Directive 2000/31/EC on electronic commerce.[72]

Concerning the facts of the case, it is worth noting that Mr Mc Fadden was running a business selling and leasing lighting and sound systems and, at the same time, operating a wireless local area network free of charge in the proximity of his business by means of a telecommunications service. It should be highlighted that access to his network was intentionally not protected in order to attract the attention of customers nearby to his business. Additionally, Mr Mc Fadden made available to the public a piece of musical work in the absence of rightholders' consent (pertaining to Sony Music). In this respect, Mr Mc Fadden denied having infringed copyright law concerning the phonogram and accepted the possibility that one of his wireless network users might have committed the violation.

From a procedural standpoint, Sony Music formally notified Mr Mc Fadden to respect their rights concerning the musical work. Failing this, Mr Mc Fadden submitted an action for a negative declaration ('negative *Feststellungsklage*') and, in turn, Sony Music brought several counterclaims in order to obtain from Mr Mc Fadden (i) payment of damages in virtue of his liability copyright law infringement, (ii) an injunction against the infringement

68 Case C-516/17 *Spiegel Online GmbH v Volker Beck*, EU:C:2019:625, § 42.

69 Case C-469/17 *Funke Medien NRW GmbH v Bundesrepublik Deutschland*, EU:C:2019:623, § 70.

70 Case C-476/17 *Pelham GmbH, Moses Pelham, Martin Haas v Ralf Hütter, Florian Schneider-Esleben*, EU:C:2019:624, § 32.

71 Case C-484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH*, EU:C:2016:689.

72 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1.

of its rights on pain of a penalty and (iii) reimbursement of the costs of giving formal notice and court costs. The court of first instance delivered a judgment by default of Mr Mc Fadden and decided in favour of Sony Music. Mr Mc Fadden appealed, invoking exemption of liability, whereas Sony Music invoked in defence the direct liability of the claimant and, subsidiarily, his indirect liability. At this point, the national court, ie *Landgericht München I* (Regional Court, Munich I, Germany), stayed the proceedings and referred the matter to the CJEU.

To begin with, the Opinion of Advocate General Szpunar is worth examining from the perspective of the human rights that were involved.[73]

First, by means of this opinion, the AG acknowledged once again the threefold conflict of rights and, implicitly, of values triggered by the case at hand, namely copyright protection as opposed to freedom of expression and information and the freedom to conduct business, enshrined in Articles 11 and 16 CFR.[74] Thus, the AG recalled the well-known weighing of interests exercise: 'Since those fundamental rights are restricted in order to give effect to the right to the protection of intellectual property enshrined in Article 17(2) of the Charter, it is necessary when restricting them to strike a fair balance between the fundamental interests involved'.[75]

Second, AG Szpunar made some noteworthy observations as regards Internet access and its wide contemporary usage. In this respect, the AG outlined the measures available for Mr Mc Fadden and examined one of them, namely password-protecting the network. It is interesting that, from this point of view, securing access to a Wi-Fi network through a password is qualified as a measure restricting freedom of expression and information. Bearing this in mind, the AG states that 'the imposition of an obligation to make access to a Wi-Fi network secure, as a means of protecting copyright on the Internet, would not be consistent with the requirement for a fair balance to be struck between, on the one hand, the protection of the intellectual property rights enjoyed by copyright holders and, on the other, that of the freedom to conduct business enjoyed by providers of the services in question'.[76]

It is also noteworthy that Internet access is assessed from the perspective of a Wi-Fi network's social benefits: '[…] any general obligation to make access to a Wi-Fi network secure, as a means of protecting copyright on the Internet, could be a disadvantage for society as a whole and one that could outweigh the potential benefits for rightholders'.[77] In this respect, the AG also led a brief copyright risk assessment and argued that infringements are highly unlikely in view of the technical properties of the network and affirmed that these

[73] Case C-484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH*, Opinion of AG Szpunar, EU:C:2016:170.

[74] *Mc Fadden v Sony Music Entertainment Germany GmbH*, Opinion of AG Szpunar, § 111.

[75] *Mc Fadden v Sony Music Entertainment Germany GmbH*, Opinion of AG Szpunar, § 112.

[76] *Mc Fadden v Sony Music Entertainment Germany GmbH*, Opinion of AG Szpunar, § 147.

[77] *Mc Fadden v Sony Music Entertainment Germany GmbH*, Opinion of AG Szpunar, § 148.

were clearly outweighed by 'the great potential for innovation', therefore imposing careful examination of the analysed measures.[78]

Surprisingly, the CJEU did not share the same perspective as the AG regarding the content of the injunction. Obviously, the Luxembourg Court agreed with the AG regarding the existence of the threefold conflict of rights at stake:

> […] in so far as such an injunction, first, places a burden on the access provider capable of affecting his economic activity and, second, is capable of restricting the freedom available to recipients of such a service from benefiting from access to the internet, the Court finds that the injunction infringes the former's right of freedom to conduct a business, protected under Article 16 of the Charter, and the right of others to freedom of information, the protection of which is provided for by Article 11 of the Charter.[79]

In this context, the CJEU recalled the applicable test, ie the balance of rights examination.[80] Bearing in mind the developments put forth in *UPC Telekabel Wien* as to the indeterminate content of the injunction, subject to a series of conditions, the Court assessed the options available to Mr Mc Fadden, namely examining all communications passing through an Internet connection, terminating that connection, or password-protecting it, and removed from the alternatives the first two due to their incompatibility with provisions of the Directive on electronic commerce and the freedom to conduct business, respectively. Thus, as regards the last of the measures, the Court noticed that 'such a measure is capable of restricting both the freedom to conduct a business of the provider supplying the service of access to a communication network and the right to freedom of information of the recipients of that service'.[81]

With regard to freedom to conduct business, the Court found no essential damage thereof, noticing that adding a password security method actually consists of 'marginally adjusting one of the technical options open to the provider in exercising its activity'.[82] As regards freedom of expression, the Court embraced a similarly pragmatic approach in stating that the essence of the right to freedom of information of the recipients of an Internet network access service remains intact since access to such a network is only one of several methods of accessing the Internet, and the measure *per se* does not block any website.[83] Therefore, the Court interpreted the addressed provisions as allowing for an injunction that imposes a password to protect the Wi-Fi network.

---

78 *Mc Fadden v Sony Music Entertainment Germany GmbH*, Opinion of AG Szpunar, para. 149.
79 *Mc Fadden v Sony Music Entertainment Germany GmbH*, § 82.
80 *Mc Fadden v Sony Music Entertainment Germany GmbH*, § 83.
81 *Mc Fadden v Sony Music Entertainment Germany GmbH*, § 90.
82 *Mc Fadden v Sony Music Entertainment Germany GmbH*, § 91.
83 *Mc Fadden v Sony Music Entertainment Germany GmbH*, § 92, 94.

To sum up, this case outlines an intriguing configuration of the threefold conflict of competing rights, copyright protection, freedom of expression and freedom to conduct business. This time, too, the Court took a slightly different approach than the AG regarding the scope of the right to information. While the AG embraced a wider interpretation of freedom of expression in view of the network users, the Court took a more pragmatic stance regarding the concrete configuration of human rights. At first glance, the interpretation of the Court appears to be rather in favour of the economic dimension of the Union and its citizens. Even if it may seem detrimental to human rights' development, the attentive analysis of the case reveals the fact that the Court actually chose the wiser path, *aurea mediocritas*, according to which human rights shall not be idealised, yet are respected with due regard to the entire ecosystem of the Union.

In light of these observations, it is legitimate to wonder whether general criteria regarding limitations on Internet access may be developed.

IV Potential Limitations

While the assessed cases outline particular solutions, it is worth examining whether a coherent view connecting the perspectives from Strasbourg and Luxembourg might be observed.

One landmark case concerning potential limitations of Internet access is *Ahmet Yildirim v Turkey*.[84] In this instance, the applicant owned and ran a website created and hosted using Google Sites, on which he published his academic work and his views on various topics. In the context of criminal proceedings, a certain offending website was blocked as a result of a judicial order. Since the owner of the impugned website did not have a service certificate and lived abroad, the court varied its blocking order the following day so that all access to Google Sites was blocked, including the applicant's website.

In this case, the ECtHR examined the request from the perspective of Article 10 ECHR, ie freedom of expression in its component of receiving and imparting information and ideas, and found a violation thereof.[85] To this aim, the Court assessed the legal effects of the preventive judicial order and acknowledged that 'the measure did not, strictly speaking, constitute a wholesale ban but rather a restriction on Internet access which had the effect of also blocking access to the applicant's website'.[86] Bearing in mind the domestic legal framework, the ECtHR underscored that the applicant's freedom of expression was subject to a form of prior restraint on the part of the public authorities and summarised the legal

[84] *Ahmet Yildirim v Turkey*, no. 3111/10, 18 December 2012 ECHR.

[85] The applicant also invoked, *inter alia*, an alleged infringement of Articles 6, 7 and 13 of the ECHR and Article 2 of Protocol No. 1, hence of his right to education, yet the ECtHR deemed it unnecessary to rule separately on either the admissibility or the merits of the ancillary complaints.

[86] *Ahmet Yildirim v Turkey*, § 54.

debate regarding 'whether, at the time the blocking order was issued, a clear and precise rule existed enabling the applicant to regulate his conduct in the matter'.[87] The Court ruled that this state measure did not fulfil the foreseeability requirements stemming from the Court's case law, noticing that Google Sites was held liable, indirectly, for a website that it hosted.

The ECtHR's reasoning relied on the fact that (i) the national notion of 'publication' covered neither the applicant's website nor Google Sites, (ii) neither Google Sites nor the applicant's website was the subject of judicial proceedings, (iii) the relevant national legal framework did not provide for a wholesale blocking of access, (iv) nor for the blocking of an entire Internet domain like Google Sites and last, (v) Google Sites was not notified regarding the illegal content being hosted and did not refuse compliance with the legal measure ordered in the criminal case.[88] Furthermore, the Strasbourg Court took note of the arbitrary conduct of the administrative body that implemented the blocking order, which 'could request the extension of the scope of a blocking order even though no proceedings had been brought against the website or domain in question and no real need for wholesale blocking had been established'[89] and whose recommendation served as the legal basis for the judicial decision without any other weighing of the interests at stake.

In its analysis, the Strasbourg Court took into account the role of the Internet and its contemporary connection to freedom of expression, as established in *Times Newspapers Ltd v the United Kingdom (nos. 1 and 2)*. In addition, it highlighted some guidelines that should have been taken into account by the domestic authorities, namely the effects of the preventive measure, that is, 'rendering large quantities of information inaccessible, [which] substantially restricted the rights of Internet users and had a significant collateral effect'.[90] All aspects factored in, the Court concluded that

> […] the measure in question produced arbitrary effects and could not be said to have been aimed solely at blocking access to the offending website, since it consisted in the wholesale blocking of all the sites hosted by Google Sites. Furthermore, the judicial review procedures concerning the blocking of Internet sites are insufficient to meet the criteria for avoiding abuse, as domestic law does not provide for any safeguards to ensure that a blocking order in respect of a specific site is not used as a means of blocking access in general.[91]

It is noteworthy that the Court's findings regarding Internet blocking, more specifically domain blocking, appear to represent the solution to a specific issue. Still, the approach is cautious, as the arguments put forth by the Court and its line of reasoning leave no room for generalisation in this matter. In this respect, solely the concurring opinion of Judge Pinto de

[87] *Ahmet Yildirim v Turkey*, § 60.
[88] *Ahmet Yildirim v Turkey*, §§ 61–62.
[89] *Ahmet Yildirim v Turkey*, § 64.
[90] *Ahmet Yildirim v Turkey*, § 66.
[91] *Ahmet Yildirim v Turkey*, § 68.

Albuquerque embraced an academic line of thought and went beyond the concrete facts of the case in formulating a series of criteria to be applied to Internet blocking measures. Since this opinion is not agreed upon by the members of the Court, its binding force cannot serve as an authoritative argument. Still, for theoretical purposes, it is advisable to highlight that the eleven criteria developed therein rely on a series of CoE-based documents referring to freedom of expression on the Internet. Thus, bearing in mind the occasion envisaged by this collateral Internet blocking, the following view in the concurring opinion appears relevant:

> […] Thus, any indiscriminate blocking measure which interferes with lawful content, sites or platforms as a collateral effect of a measure aimed at illegal content or an illegal site or platform fails *per se* the "adequacy" test, in so far as it lacks a "rational connection", that is, a plausible instrumental relationship between the interference and the social need pursued. […] When exceptional circumstances justify the blocking of illegal content, it is necessary to tailor the measure to the content which is illegal and avoid targeting persons or institutions that are not *de jure* or *de facto* responsible for the illegal publication and have not endorsed its content. In the case of *interim* or preventive measures which are based on reasonable grounds to suspect the commission of a crime, freedom of expression warrants not only a particularly tight legal framework ("*cadre légal particulièrement strict*") but also the most careful scrutiny by the courts, and consequently the exercise of special restraint.

As examined above, the potential limitations on Internet access are approached distinctly at the EU level, given the prevalently economic dimension of the Union. Thus, restrictions concerning certain websites, as was the case in *UPC Telekabel Wien*, or to Internet access in Wi-Fi format, as the facts unfolded in *Mc Fadden*, are assessed from the point of view of the restricted rights, namely freedom of expression or freedom to conduct business in a comparable manner to that applied by the ECtHR. In this respect, the similarity stems from Article 52(3) of CFR, which established quite clearly that the ECHR provisions constitute a minimum threshold of protection.[92]

Indeed, case law proves that the Luxembourg perspective overlaps significantly with the Strasbourg point of view. For instance, in *Pelham and Others*, the Luxembourg Court applied the weighing of interests test with reference to the freedom of expression as enshrined in both CFR and ECHR, making clear the connection with the ECtHR's case law.[93] A similar coherence of perspective may be identified in *Funke Medien NRW*, where

[92] EU Charter of Fundamental Rights Article 52(3): 'In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.'

[93] *Pelham GmbH, Moses Pelham, Martin Haas v Ralf Hütter, Florian Schneider-Esleben*, § 34: 'A balance must be struck between that right and other fundamental rights, including freedom of the arts, enshrined in Article 13 of the Charter, which, in so far as it falls within the scope of freedom of expression, enshrined in Article 11 of the Charter and in Article 10(1) of the European Convention for the Protection of Human Rights

Luxembourg clarified that its exercise of balancing the interests at stake in matters referring to freedom of expression is, in principle, equivalent in scope to the examination applied by the ECtHR.[94] In this last case, the Court underlined the exact legal relation between the rights enshrined in the CFR and ECHR:

> […] it should be noted that in so far as the Charter contains rights which correspond to those guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950 ('the ECHR'), Article 52(3) of the Charter seeks to ensure the necessary consistency between the rights contained in it and the corresponding rights guaranteed by the ECHR, without thereby adversely affecting the autonomy of EU law and that of the Court of Justice of the European Union […] Article 11 of the Charter contains rights which correspond to those guaranteed by Article 10(1) of the ECHR […].[95]

Scholars have also noticed the interconnection between the ECtHR and CJEU levels of protection granted to equivalent safeguarded rights and freedoms, highlighting that the standard of protection granted by the ECHR and, accordingly, by the Court in its interpretation, constitutes only a minimum threshold, regardless of the effective reference to specific cases of the ECtHR.[96] In this respect, it has been observed that 'the jurisprudence of the two courts is complementary, as the ECtHR approaches the problems on human rights grounds, while the CJEU approaches them on economic grounds'.[97] Still, in both cases, the impact of technology on human rights is perceived as a threat rather than an opportunity.[98]

In this respect, the following observation appears accurate as far as the right to Internet access in concerned: 'although the ECtHR and the CJEU differ on certain issues, this is not surprising, as the two courts examine the same issues from different angles. […] The complementary jurisprudence of the two international courts contributes significantly to ensuring that the liability of platform providers and the internet as a complex and constantly changing ecosystem is on a more solid footing in the practice of national courts.'[99]

Strictly referring to limitations to Internet access, scholars have put forward a series of conditions to be verified *in concreto* for each and every such restrictive measure. These criteria refer to:

---

and Fundamental Freedoms, signed at Rome on 4 November 1950, affords the opportunity to take part in the public exchange of cultural, political and social information and ideas of all kinds.'

94 *Funke Medien NRW GmbH v Bundesrepublik Deutschland*, §§ 73–74.

95 *Funke Medien NRW GmbH v Bundesrepublik Deutschland*, § 73.

96 Amelia-Raluca Onișor, 'CJUE, Carta și CEDO. Amurgul unei relații atipice?' (2021) (1–2) Revista Themis 179.

97 Gosztonyi (n 24) 141.

98 Pollicino (n 14) 193.

99 Gosztonyi (n 24) 142.

> First, legislation should provide for measures that can be used to restrict, and should also set out in clear and predictable rules what content can be blocked and to what extent. In determining what content can be blocked, national legislation should follow the standards set by international human rights law. Second, blocking measures should be ordered by a court or an independent judicial body. Non-independent governmental bodies are likely to apply overly restrictive measures, as their primary objective is to protect interests that conflict with freedom of expression. Third, Internet users and ISPs should be able to challenge restrictive measures. To this end, when they try to access a blocked site, they should be provided with sufficient information on how to challenge the measure. Finally, to avoid blocking legitimate content, blocking measures should be strictly targeted, so IP address technologies should only be used to target non-shared IP servers.[100]

Bearing in mind the Strasbourg-Luxembourg link, in terms of judicial interpretation, it can be concluded that the same criteria shall be applied for restrictions to Internet access pursuant to EU legal instruments. Still, given the more pragmatic view embraced by the CJEU in cases such as *Mc Fadden*, with regard to the Union's human rights dimension, distinct approaches are to be expected. However, these differences appear to be predictable and natural since they seem to be included in the greater architecture of the European *lato sensu* system of human rights protection.

V Conclusions

The debate concerning the autonomous or implicit existence of the right to Internet access is far from settled, especially since the case law of the judicial centres of the Union's space seems to leave a certain leeway for the explicit recognition of this right. The ECtHR case law assessed here reveals that the Strasbourg Court has duly reacted to the new technological framework that underpins several Convention-protected rights. Not only did the Court acknowledge the societal role of the Internet at a general level, but it also analysed its dimensions in connection with alleged violations of conventional rights and freedoms. The bipartite 'balancing test' was used to oppose the safeguarded right and competing interests. Thus, in *Kalda v Estonia*, in *Jankovskis v Lithuania* and then later in *Ramazan Demir v Turkey*, the right to receive and impart information was assessed from a contemporary perspective of those deprived of liberty. Therefore, the acknowledgement of the need for Internet access appeared to apply to a specific category of individuals. Having found violations of Article 10 of the ECHR in all these cases, the Strasbourg Court highlighted the significant role of Internet access in factual situations which occurred over 15 years ago. While these findings may not be generalised, the analysed case law leaves room for future

[100] Gosztonyi (n 24) 155.

jurisprudential developments insofar as our society's *status quo* has dramatically changed in favour of a higher degree of technology usage and greater expectations of connectivity.

As regards the case law of the CJEU, the human rights debate emerges in the context of a differently designed conflict of values. While numerous cases solved by the Luxembourg Court imply a dual exercise of balancing the rights and interests at stake, a few helped an intriguing and more complex examination. It is the case of national injunctions on various grounds and legal instruments that gives rise to legal developments that shed light on the threefold conflict of values thus triggered. Hence, in *UPC Telekabel Wien*, the Court assessed human rights in its discussion and focused on freedom of expression. Thus, the right to Internet access was thoroughly analysed through the lens of freedom of expression, with no reference to its severability, that is, its status of a stand-alone human right. Similarly, in *Mc Fadden*, the CJEU chose once again the solution it deemed suitable for reconciling all the values at stake. Using a rather pragmatic approach, the Court chose to rule in favour of economic interests and took no explicit stance on the autonomy of Internet access. This apparent loss in the human rights field is actually a subtle way of promoting a practical and effective perspective on fundamental freedoms to the detriment of ideal and illusory legal categories.

Limitations to Internet access are assessed in relation to the landmark ruling in *Ahmet Yildirim v Turkey*. With regard to Internet blocking, the Strasbourg Court put forth the solution to a specific issue, stating that abusive and arbitrary measures shall, by all means, be avoided, hence imposing the judicial review of the restrictive measures. Even if no theoretical general-use observations were made, the case constitutes a bedrock for building abstract criteria for assessing such measures. Pursuant to Article 52(3) CFR, this standard of protection represents the minimum threshold conferred at the EU level. Hence, the conditions therein shall be accordingly applied in cases of Internet restriction occurring within the Union's sphere of competence.

All in all, as legal developments stand at the moment, the right to Internet access enjoys only an implicit existence due to the reluctance to acknowledge it in an independent manner. The ECtHR and CJEU case law are defined by complementarity more than mere dichotomy. Therefore, Internet access is rather a 'facilitator' of the exercise of other rights than an autonomous right. As a guiding line of this analysis, it is worth recalling the visionary considerations put forth by The Honourable Lloyd Axworthy, a prominent Canadian public figure: 'The key is how to maximize the Internet's potential for good as a tool to promote and protect human rights: its use for human rights education, as a means of organizing human rights defenders and getting information on human rights violations out to the world.'[101] Bearing these thoughts in mind, it seems legitimate to ask whether it is (high) time for a change of perspective and to what extent academia or other stakeholders should take some braver steps in this direction.

[101] Hick, Halpin, Hoskins (n 3) 16.

Gergely Ferenc Lendvai*

Hybrid Regimes and the Right to Access the Internet – Findings from Turkey and Russia in the Context of the Judgments of the European Court of Human Rights

Abstract

The liaison between authoritarian political governance and Internet access is complex, particularly in hybrid regimes like Turkey and Russia. This paper focuses on the right to access the Internet as perceived by European Court of Human Rights (ECtHR) case law involving the two aforementioned countries, examining the balance between political interests and individual rights. Through comprehensive case comparisons, the present research outlines tensions between European human rights principles and the actions of hybrid regimes. The paper's focal point lies in examining multiple landmark cases from Turkey and Russia to trace the evolution of ECtHR judgments on Internet freedom. Moreover, the paper reflects on broader implications, questioning whether ECtHR decisions enhance individual rights protection in the digital age and suggests avenues for improving Internet governance in hybrid regimes through international legal mechanisms. The paper is methodologically founded on a comprehensive literature review and legal case comparisons. The findings reveal a critical endangerment of right to access the Internet, most notably in Russia, whose withdrawal from the European Convention on Human Rights exacerbates concerns over freedom of expression and digital rights protection. In Turkey, frequent Internet blockages and legal reforms continue to erode digital freedoms. This research proposes that, despite ECtHR's rulings aimed at reinforcing individual rights, the broader implications remain unresolved as hybrid regimes persistently challenge and undermine the principles of human rights protection in the digital age.

* Dr Gergely Ferenc Lendvai, PhD Candidate, Pázmány Péter Catholic University and Research Fellow at the University of Richmond. This paper was supported by the Rosztoczy Foundation Scholarship, the project 149657_ADVANCED_24 provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund and the Hungarian Hungarian State Eötvös Scholarship. ORCID iD: 0000-0003-3298-8087.

Keywords: human rights, European Court of Human Rights, Turkey, Russia, right to access the Internet, digital divide, hybrid regimes

I Introduction

As the Internet has become the primary source for imparting and receiving information, one could confidently state that those who can access it can access the world itself. An integral and, much rather, inherent segment of our lives, the Internet allows users to communicate with friends and colleagues, shop, create, generate and consume content and work like never before in history. As Merten Reglitz states, however, in our affluent world, Internet access is so readily available that it is easy to forget how fundamentally it shapes our lives.[1] Nonetheless, it is even easier to forget how evident and given it seems, especially for those living in the Global North, that one has access to the Internet all of the time. The present research focuses on a very different Internet experience: one which can be understood within the theoretical and practical frameworks of censorship,[2] state supervision, propaganda,[3] disregard for minorities and their rights, and the suppression of political and religious views.

The paper's primary focus lies in understanding challenges related to the right to access the Internet (RATI) in two countries, often described as hybrid regimes,[4] Turkey and Russia. To support the examination, the research is structured in a tripartite manner. First, the term 'hybrid regimes' is conceptualised using the pertaining academic literature. At this point, I examine how and why both Turkey and Russia may be regarded as hybrid regimes, and I introduce the principal concerns related to Internet usage, access and coverage in a hybrid political system. Second, to contextualise the theoretical background, multiple key cases involving the case law of the European Court of Human Rights (ECtHR or Court) in which either Turkey or Russia was the respondent party will be examined and highlighted. These cases serve as the core of the study, as the Court has underlined a myriad of principles guiding the judgments concerning the right to access the Internet. This segment covers crucial cases involving Article 10 of the European Convention of Human Rights (ECHR)

---

1 Merten Gerlitz, 'The Human Right to Free Internet Access' (2019) 37 (2) Journal of Applied Philosophy 314, DOI: https://doi.org/10.1111/japp.12395

2 Gergely Gosztonyi, *Censorship from Plato to Social Media. The Complexity of Social Media's Content Regulation and Moderation Practices* (Springer 2023, Cham) 147–168, DOI: https://doi.org/10.1007/978-3-031-46529-1_10

3 Gergely Ferenc Lendvai, 'Media in War: An Overview of the European Restrictions on Russian Media' (2023) 3 (3) European Papers, DOI: https://doi.org/10.15166/2499-8249/715

4 Ole Frahm and Katharina Hoffmann, 'Dual Agent of Transition: How Turkey Perpetuates and Challenges Neo-Patrimonial Patterns in Its Post-Soviet Neighbourhood' (2020) 37 (1) East European Politics 110, DOI: http://dx.doi.org/10.1080/21599165.2020.1733982

from the *Cengiz* judgment,[5] a case concerning the wholesale blocking of the very large online platform YouTube for *Kharitonov* and related cases in Russia[6] involving collateral blockings of multiple highly frequented websites. The examination aims to synthesise the findings of the ECtHR and highlight the guiding principles concerning the right to access the Internet. To provide a critical view of the above, the paper also includes perspectives about the future of the right to access the Internet in Turkey and Russia. This section underlines the possible detrimental impacts of digital authoritarianism in the online sphere, an expression used to describe the hindering of human rights, especially freedom of expression, on the Internet.[7]

The present paper aims to contribute to the legal scholarly reception concerning the right to access the Internet and the polemics of hybrid regimes and their liaison with the Internet. A further objective of the study is to amplify the discourse on the issues in hybrid political systems and foster discourse on the possibilities to mitigate the risks thereof. Last, this paper aims to contribute to the ongoing research on discriminatory Internet access cases and the ever-developing legal literature on the relationship between censorship and the role of the Internet as the primary field where one can express oneself.

II Conceptualisation of Hybrid Regimes and their Relation to Freedom of Expression Online

'Is Russia a democracy?' commences Larry Diamond in his study on hybrid regimes.[8] Despite the simplicity of the question, providing an answer involves issues of near-unimaginable complexity; from *pseudodemocracies*[9] to the historical essence of liberal democracies,[10] hybrid regimes question the fundamentals of what it means for a society to be democratic, free and open. To lay the foundation for the investigation of the case of access to the Internet in Turkey and Russia, it is essential first to conceptualise what it means to be a hybrid regime. According to Ali Riaz, who refers to Terry Linn Karl, one of the first scholars to define the phenomenon,[11] hybrid regimes are best described as grey areas between

5 *Cengiz and Others v Turkey*, nos. 48226/10, 14027/11, ECHR, 1 December 2015.

6 *Vladimir Kharitonov v Russia*, no. 10795/14, ECHR, 23 June 2020.

7 Richard Ashby Wilson, 'The Anti-Human Rights Machine: Digital Authoritarianism and The Global Assault on Human Rights' (2022) UCONN Faculty Articles and Papers 614.

8 Larry Diamond, 'Thinking About Hybrid Regimes' (2002) 13 (2) Journal of Democracy 21, DOI: https://doi.org/10.1353/jod.2002.0025

9 Petra Bárd, Laurent Pech, 'How to Build and Consolidate a Partly Free Pseudo Democracy by Constitutional Means in Three Steps: The 'Hungarian Model' Reconnect Europe Working Paper 2019/4, DOI: https://doi.org/10.2139/ssrn.3608784

10 T. F. Rhoden, 'The liberal in liberal democracy' (2013) 22 (3) Democratization 3, DOI: https://doi.org/10.1080/13510347.2013.851672

11 Terry Lynn Karl, 'The Hybrid Regimes for Central America' (1995) 6 (3) Journal of Democracy 72–87, DOI: https://doi.org/10.1353/jod.1995.0049

consolidated democracy and blatant authoritarianism.[12] Though definitions vary depending on theoretical orientations,[13] an illustrative and guiding conceptualisation that can be interconnected with the definition of *Karl* and *Riaz* comes from *Leonardo Morlino,* whose definition has been cited in many articles on the issue. *Morlino* describes hybrid regimes as

> A set of institutions that have been persistent, be they stable or unstable, for about a decade, have been preceded by authoritarianism, a traditional regime (possibly with colonial characteristics), or even a minimal democracy and are characterised by the break-up of limited pluralism and forms of independent, autonomous participation, but the absence of at least one of the four aspects of a minimal democracy.[14]

Whether Turkey and Russia are hybrid regimes has been confirmed by decades of scholarly literature. Per Joakim Ekman's hybrid regime indicator and Henry E. Hale's study,[15] Russia is the blueprint of a hybrid regime, while Turkey is close to ticking all the boxes that make it a *perfect* hybrid regime.[16] To specify, Russia's status as a hybrid regime stems from its amalgamation of democratic and authoritarian traits. Despite nominal democratic processes such as periodic elections and institutional structures,[17] authority is heavily centralised under President Vladimir Putin and his close associates. The government exerts stringent control over media platforms, stifles political dissent and restricts civil liberties, creating an environment where opposition voices are marginalised and dissenters face severe consequences.[18] This hybrid nature enables the regime to project an illusion of democratic governance while consolidating authoritarian control, thereby allowing Putin's administration to suppress opposition effectively and maintain power.

In the case of Turkey, despite democratic institutions such as regular elections and a parliamentary system, power has become increasingly concentrated under President Recep Tayyip Erdoğan and the ruling Justice and Development Party (AKP). Erdoğan's government is often criticised for having gained unprecedented control over media outlets, using legal

---

12 Ali Riaz, *Voting in a Hybrid Regime* (Springer 2019, Cham) 14, DOI: https://doi.org/10.1007/978-981-13-7956-7

13 Muntasser Majeed Hameed, 'Hybrid Regimes: An Overview' (2022) 22 (1) IPRI Journal 5, DOI: https://doi.org/10.31945/iprij.220101

14 Leonardo Morlino, 'Are There Hybrid Regimes? Or Are They Just an Optical Illusion?' (2009) 1 (2) European Political Science Review 273, DOI: http://dx.doi.org/10.1017/s1755773909000198

15 Henry E Hale, 'Eurasian Polities as Hybrid Regimes: The Case of Putin's Russia' (2010) 1 (1) Journal of Eurasian Studies 33, DOI: http://dx.doi.org/10.1016/j.euras.2009.11.001

16 Joakim Ekman, 'Political Participation and Regime Stability: A Framework for Analyzing Hybrid Regimes' (2009) 30 (1) International Political Science Review 7, DOI: http://dx.doi.org/10.1177/0192512108097054

17 Luke March, 'Managing Opposition in a Hybrid Regime: Just Russia and Parastatal Opposition' (2009) 68 (3) Slavic Review 504, DOI: http://dx.doi.org/10.1017/s0037677900019707

18 J Paul Goode, 'Redefining Russia: Hybrid Regimes, Fieldwork, and Russian Politics' (2010) 8 (4) Perspectives on Politics 1055, DOI: http://dx.doi.org/10.1017/s153759271000318x

measures to suppress political opposition and imposing restrictions on civil liberties;[19] as a result, dissenting voices are being marginalised, and individuals who express dissent often face repercussions.[20]

III Cases from Turkey and Russia

The singling out of two hybrid regimes out of many is a classic case of when a research interest meets research gaps. The ECtHR case law related to the RATI presents a striking picture of how Turkey and Russia 'dominate' cases associated with RATI. Out of 13 cases directly linked to the RATI, 11 are from these two countries, and all general/blanket and content restrictions are particularly and exclusively from these two countries. The figure below presents the overall picture of ECtHR cases related to the RATI.

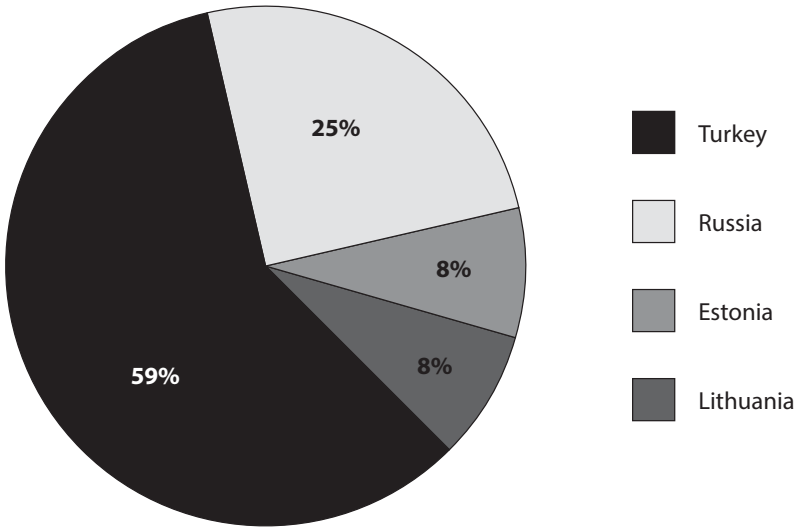


Figure 1: Statistics concerning countries involved in cases related to the RATI before the ECtHR as of 28 March 2024 (Source: Own editing)

Furthermore, the ECtHR's cases related to RATI involving Turkey and Russia may be divided into two major categories with three subcategories as could be seen in the following table.

[19] Nate Schenkkan and Aykut Garipoglu, 'Turkey Elections 2023: How Erdogan and the AKP Could Rig the Vote' (May 16, 2023) Foreign Policy, <https://foreignpolicy.com/2023/05/03/turkey-elections-erdogan-kilicdaroglu-vote-manipulation-suppression-media/> accessed 15 October 2024.

[20] Nikolaos Stelgias, 'Turkey's Hybrid Competitive Authoritarian Regime; A Genuine Product of Anatolia's Middle Class' (2015) 4 (2) The Levantine Review 2, DOI: https://doi.org/10.6017/lev.v4i2.9161

Table 1: Distribution of cases before the ECtHR concerning RATI (Source: Own editing)

Cases related to RATI before the ECtHR		
Internet access-blocking measures		Restrictions on Prisoners' RATI
Wholesale/blanket blockings	Content blocking	
• Ahmet Yıldırım v Turkey • Akdeniz v Turkey • Cengiz and Others v Turkey • Vladimir Kharitonov v Russia, OOO Flavus and Others v Russia, Bulgakov v Russia and Engels v Russia • Wikimedia Foundation, Inc. v Turkey • Taganrog LRO and Others v Russia	• Kablis v Russia • Akdeniz and Altiparmak v Turkey no. 1 (pending) • Akdeniz and Altiparmak v Turkey no. 2 (pending)	• Ramazan Demir v Turkey • Mehmet Reşit Arslan and Orhan Bingöl v Turkey

In the following segments, short summaries of the cases will be presented, followed by a critical analysis of and lamentation about the future of RATI in Turkey and Russia. As the paper's objective is to cover the specific cases of wholesale blockings and the complete restriction of the RATI, these cases will be analysed solely. However, as not many scholars have covered the particular issues regarding content blockings, and cases regarding the RATI of prisoners before the ECtHR have only been recently examined by Gergely Gosztonyi and Gergely Ferenc Lendvai,[21] this paper also serves as an exposition of the prevailing European jurisprudential landscape concerning the RATI, offering a comprehensive portrayal of its nuanced doctrinal intricacies.

1 *Ahmet Yıldırım v Turkey*[22]

The first ECtHR case to deal with the issue of RATI was the *Ahmet Yıldırım v Turkey* case. Per the facts of the case, Turkish national Ahmet Yıldırım owned a website hosted by the Google Sites service. The applicant published his academic writings and articles on the site as well as opinion pieces on various issues.[23] In June 2009, the Denizli Criminal Court of First Instance issued an order to block an Internet site accused of insulting the memory of

[21] Gergely Ferenc Lendvai, Gergely Gosztonyi, 'Access Denied – interpreting the digital divide by examining the right of prisoners to access the Internet in the case law of the European Court of Human Rights' (2024) 17 (1) Baltic Journal of Law & Politics 223–237, DOI: https://doi.org/10.2478/bjlp-2024-0011

[22] *Ahmet Yildirim v Turkey*, no. 3111/10, 18 December 2012 ECHR.

[23] *Ahmet Yıldırım v Turkey* § 7.

Mustafa Kemal Atatürk, founder of the Turkish Republic, as part of the preventive measures imposed during the ongoing criminal proceedings against the disputed site's owner.[24] The Telecommunications Directorate (PIT) was tasked with executing this order.[25] Subsequently, the PIT requested that the court expand the scope of the order to block access to the entirety of Google Sites on which both the respective site and another owned by the applicant were hosted.[26] The PIT argued that this was necessary as the owner of the offending site resided abroad, making it challenging to block just that specific site.

Consequently, access to all of Google Sites was blocked, including Mr. Yıldırım's site. Despite the applicant's attempts to resolve the issue, the court's blocking order persisted and by April 2012, the applicant was still unable to access his own website. He noted that, to his knowledge, the criminal proceedings against the owner of the offending site had been halted due to the inability to ascertain the accused's identity and address, particularly since the latter lived outside the country.[27] The applicant challenged the national courts' decision before the ECtHR.

The applicant alleged a violation of his right to freedom of information under Article 10 of the ECHR due to the blocking of Google Sites, which he argued amounted to indirect censorship. He contended that the repercussions were disproportionate and criticised the lack of fairness and impartiality in the blocking process. Though the Government did not respond, the Open Society Justice Initiative (OSJI) intervened, likening the blocking to prior restraint and cautioning against the risks of 'collateral censorship'. They highlighted the absence of safeguards against arbitrariness in the Turkish system, resulting in numerous prolonged blockades of platforms like YouTube and Google services without adequate oversight. This contrasted with practices in France, Germany and the UK, where more targeted blocking measures had been implemented.

The ECtHR recognised the applicant's ownership and usage of a website for publishing academic work and views associated with various fields. The Court emphasised that while Article 10 of the ECHR does not prohibit prior restrictions on publication outright, it also stressed the need for the meticulous scrutiny of such measures due to their inherent risks. This is especially critical for press freedom, as delays in publication can render information obsolete and diminish its value.[28] Highlighting the significance of websites in fostering freedom of expression, the Court referenced previous rulings[29] that emphasised the role of the latter in facilitating public access to news and information. It noted that Google Sites, a

[24] *Ahmet Yıldırım v Turkey* § 8.
[25] *Ahmet Yıldırım v Turkey* § 9.
[26] *Ahmet Yıldırım v Turkey* § 10.
[27] *Ahmet Yıldırım v Turkey* § 14.
[28] *Ahmet Yıldırım v Turkey* §§ 46–47.
[29] cf *Times Newspapers Ltd v the United Kingdom* (dec.), nos. 3002/03 et 23676/03, ECHR 2009, § 27.

platform enabling website creation and sharing, constitutes a means of exercising freedom of expression.[30]

The Court highlighted the nature of the case's central issue as the collateral impact of a preventive measure adopted in a judicial proceeding. Despite Google Sites and the applicant's site not being directly involved, the PIT blocked access to both sites to enforce a measure ordered by the Denizli Criminal Court. This constituted a form of prior restraint, occurring before a judgment on the merits. The Court deemed such a measure intended to affect Internet accessibility as triggering the defending state's liability under Article 10. The contested blocking resulted from an initial ban on a third-party website, which extended to Google Sites, which affected the applicant's website hosted on the same domain. Despite the limited scope, the restriction significantly curtailed Internet access, impacting the exercise of freedom of expression and information. Consequently, the Court concluded that the measure constituted the interference of public authorities with the individual's right to freedom of expression, including the freedom to receive and communicate information or ideas.

Applying the three-part cumulative test, the Court emphasised that the phrase 'prescribed by law' in Article 10(2) implied not only that the impugned measure must have had a basis in domestic law but also pertained to the quality of the law itself. It required the accessibility of the law to the individual concerned, who must have been able to foresee its consequences and its compatibility with the rule of law. In this case, the Court observed that blocking access to the website involved in the judicial procedure had a legal basis, namely Article 8(1) of Law No. 5651. However, the applicant argued that Article 8(1) did not meet the requirements of accessibility and foreseeability, alleging its uncertainty. The question at stake was whether, at the time the blocking decision was made, there existed a clear and precise norm that would enable the applicant to regulate his conduct accordingly. The Court noted that under Article 8(1) of Law No. 5651, a judge could order blocking access to Internet publications if there were sufficient grounds to suspect that they constituted offences. However, neither the applicant's website nor Google Sites per se was the subject of a judicial procedure under Article 8(1).

Moreover, there was no indication that the law allowed for the blocking of an entire Internet domain, such as Google Sites. Furthermore, the Court observed that Article 8(3) and (4) of Law No. 5651 granted extensive powers to an administrative body (the PIT) in executing a blocking decision initially adopted for a specific site. In summary, the Court found that Article 8 of Law No. 5651 did not meet the Convention's foreseeability requirement and lacked protection for the applicant, constituting a violation of Article 10.

[30] *Ahmet Yıldırım v Turkey* § 49.

2 *Akdeniz v Turkey*[31]

On 26 June 2009, the Beyoğlu Public Prosecutor's Office, upon a request from the MÜYAP (Professional Union of Phonogram Producers), decided to block access to 'myspace.com' and 'last.fm' due to alleged copyright violations. Based on Article 4 of Law No. 5846 on artistic and intellectual works, the decision required Internet providers to suspend services within three days, with a seven-day window for opposition.[32] No opposition was lodged by the affected websites or their providers by the deadline. On 29 September 2009, the applicant, Yaman Akdeniz, a user of the aforementioned sites, contested the decision, arguing it infringed his right to information access. He claimed the sites hosted lawful content and constituted vital platforms for the freedom of expression. He also challenged the constitutionality of the relevant law.[33] The Beyoğlu Criminal Court (BCC) dismissed the applicant's claim the next day (30 September), citing his lack of standing and the decision's compliance with legislation. On 5 October 2009, the applicant appealed before the Chamber of Copyright Matters of the BCC (CCBCC).

The applicant's argument centred on the disproportionate nature of the blocking measure, which affected lawful content. He contended that the law lacked clarity and precision regarding its application to Internet platforms. The CCBCC upheld the decision on 12 October 2009, emphasising the necessity of blocking to combat copyright infringement, especially given the global reach of Internet piracy. It has been noted that before requesting the blocking, MÜYAP issued warnings to the affected sites to cease the unauthorised distribution of copyrighted works. However, as the sites did not comply, the public prosecutor ordered the blocking based on expert reports submitted by MÜYAP. The chamber concluded that blocking access to sites engaged in widespread distribution of copyrighted works was the only effective means to protect copyrights, particularly given the prevalence of Internet piracy. It emphasised that since the Internet infrastructure did not allow for selective blocking of site content, a general block was necessary to protect copyrights effectively. The chamber also rejected the argument regarding the alleged unconstitutionality of additional Article 4 of the law on artistic and intellectual works.[34] The applicant challenged the decision before the ECtHR.

The Court first examined whether the applicant could claim to be a victim of a Convention violation due to the website-blocking measure. It reiterated that the notion of 'victim' under Article 34 of the Convention must be interpreted autonomously, irrespective of internal concepts such as interest or standing to act.[35] This primarily concerns those directly affected by the alleged interference. The Court has previously accepted, albeit

[31] *Akdeniz v Turkey* (dec.), nos. 41139/15, 41146/15, ECHR 2021-II.
[32] *Akdeniz v Turkey* §§ 2–3.
[33] *Akdeniz v Turkey* § 5.
[34] *Akdeniz v Turkey* § 8.
[35] *Akdeniz v Turkey* § 19.

exceptionally, requests from individuals indirectly affected by Convention violations. However, a link between the applicant and the alleged harm resulting from the violation must exist. In this case, the Court noted that by a decision made on 26 June 2009, the media section of the Beyoğlu Public Prosecutor's Office ordered the blocking of access to the 'myspace.com' and 'last. fm' websites, citing copyright infringement. As a user of these sites, the applicant primarily complained about the collateral effect of the measure taken under the law on artistic and intellectual works. While acknowledging the importance of Internet users' rights, the Court held that the applicant's indirect exposure to the blocking of two music-sharing websites did not suffice for his recognition as a 'victim' under Article 34 of the Convention. Although he could access a variety of music through alternative means without infringing copyright rules, he did not assert that the blocked sites provided unique information of particular interest to him.[36] Furthermore, the Court distinguished this case from previous cases, such as the *Yıldırım* case, where similar measures directly affected individuals. The Court also recalled its strict scrutiny of website blocking decisions due to their potentially significant collateral censorship effects.

Consequently, the Court concluded that the applicant could not claim to be a victim of a violation of Article 10 of the Convention due to the disputed measure. The lack of victim status under Article 10 also affected the applicant's Article 6 complaint. Therefore, the application was incompatible *ratione personae* with the Convention provisions and had to be dismissed under Article 35 §§ 3 and 4 of the Convention.

3 *Cengiz and Others v Turkey*[37]

The case concerns Turkish law professors and YouTube, the most significant video-sharing platform in the world. Similarly to the facts in the Yıldırım-judgement, the Ankara Criminal Court of First Instance ordered the blocking of access to YouTube with the aim of prohibiting insults to the memory of Atatürk in ten video files on the website.[38] Cengiz and the other applicants (applicants) contested the blocking order, arguing for the right to freedom of information and emphasising the public interest in YouTube access and the disproportionate restriction on their freedom to receive information and ideas.[39] Despite these objections, the Ankara Criminal Court dismissed them, asserting that the blocking order complied with legal requirements. It maintained that while YouTube had blocked access to the files in Turkey, they remained available globally on the platform. Additionally, it has been argued that the applicants lacked standing as they were not involved in the investigation, and a

[36] *Akdeniz v Turkey* § 22.
[37] *Cengiz v Turkey* (dec.), no. 48226/10 and 14027/11, ECHR 2015.
[38] *Cengiz v Turkey* § 7.
[39] *Cengiz v Turkey* § 8.

previous dismissal of similar objections was noted.[40] After unsuccessfully exhausting all domestic remedies, the applicants challenged the blocking decision before the ECtHR.

The applicants challenged the YouTube blocking, citing a breach of their freedom of information. They argued that the blanket block disproportionately restricted access to unrelated content. The government countered, asserting the legality and necessity of blocking and aligning it with EU standards. They emphasised fair legal proceedings and recent amendments to the law while acknowledging technological limitations in implementing URL filtering for foreign-based websites in Turkey. The ECtHR revisited the fundamental principle that the Convention does not allow an *'actio popularis'*, emphasising that individuals must demonstrate they are directly or indirectly affected by a violation attributable to a Contracting state to petition the court. Drawing on precedent cases like *Yıldırım*, *Tanrıkulu* and *Akdeniz*, the ECtHR underscored the need for a nuanced assessment of each case, considering the manner in which individuals utilise the platform and the potential impact of any measures taken.[41] In this instance, the applicants, active users of YouTube, highlighted the adverse consequences of the blocking order on their academic endeavours and the significant role of the platform in their professional lives. They stressed their active engagement on YouTube as consumers and producers of content relevant to their respective fields. This active involvement resembled the scenario in the *Ahmet Yıldırım* case, where the applicant utilised his personal website to share academic work and views.[42]

Moreover, the ECtHR noted distinctions between these cases and previous rulings,[43] particularly regarding the nature of content hosted on YouTube. Unlike cases involving copyright infringement, YouTube serves as a vital platform not only for artistic content but also for political discourse and social activities. The availability of diverse and unique information on YouTube, which is not easily accessible elsewhere, further underscored its importance to the applicants. Acknowledging the Constitutional Court's recognition of victim status for active users of websites like YouTube, the ECtHR endorsed this perspective. It affirmed that the applicants' active engagement on the platform justified their claim to victim status, irrespective of whether the blocking order directly targeted them.[44]

Reviewing whether the interference was justified, the Court applied the known tripartite test.[45] When evaluating the 'prescribed by law' criteria, the Court acknowledged that while the blocking of a website had a legal basis in section 8(1) of Law no. 5651, concerns were raised regarding its accessibility and foreseeability. The applicants argued that the

---

40 *Cengiz v Turkey* § 10.

41 *Cengiz v Turkey* § 48–49.

42 Elena Lazăr and Nicolae-Dragoș Costescu, 'Romania' in Oreste Pollicino (ed), *Freedom of Speech and the Regulation of Fake News* (Intersentia 2023, Cambridge) 431–437.

43 cf *Akdeniz v Turkey.*

44 *Cengiz v Turkey* §§ 54–55.

45 Janneke Gerards, 'How to improve the necessity test of the European Court of Human Rights' (2013) 11 (2) International Journal of Constitutional Law 11.

provision lacked the necessary precision, rendering it too vague to meet the standards of foreseeability.[46] Drawing on precedent cases such as the *Yıldırım* judgment, it noted that Turkish law did not authorise the wholesale blocking of entire websites based on the content of a single page. Instead, it permitted the blocking of specific publications under certain conditions. The absence of specific statutory authorisation for such broad measures has already been highlighted, mainly when the Ankara Criminal Court of First Instance decided to block all access to YouTube.

Moreover, the ECtHR noted the absence of URL filtering technology for foreign-based websites in Turkey, leading to the wholesale blocking of entire websites as the only practical option. This approach substantially restricted Internet users' rights and had significant collateral effects, contravening the requirements of the Convention.[47] Consequently, the Court concluded that the interference resulting from the application of the pertaining national law did not meet the standard of lawfulness under the Convention, failing to provide the applicants with the requisite protection guaranteed by the rule of law in a democratic society. Therefore, the applicants' rights under Article 10 of the ECHR had been violated.

4 *Vladimir Kharitonov v Russia,*[48] *OOO Flavus and Others v Russia,*[49] *Bulgakov v Russia,*[50] *Engels v Russia*[51]

Following Dirk Voorhoof's note, the cases mentioned above are presented jointly.[52] The cases involved various types of blocking measures, such as collateral blocking, excessive blocking and wholesale blocking of media outlets, implemented under Russia's Information Act. These measures were used to block websites and online media outlets, leading to concerns regarding their arbitrary and excessive effects. The ECtHR emphasised the crucial role of the Internet in enabling freedom of expression in all four cases. To briefly summarise, in the *Kharitonov* case, the applicant discovered that the IP address of his website, Electronic Publishing News, had been blocked by the Roskomnadzor telecoms regulator. This action had been taken following a decision by the Federal Drug Control Service to block access to another website, rastaman.tales.ru, which shared the same hosting company and IP address as the applicant's website. Despite the applicant's complaint to the court, highlighting that his website contained no illegal content, the courts upheld Roskomnadzor's decision as lawful without considering its effect on the applicant's website.

---

46 *Cengiz v Turkey* §§ 60–62.

47 *Cengiz v Turkey* § 64.

48 *Vladimir Kharitonov v Russia* (dec.), no. 10795/14, ECHR 2020.

49 *OOO Flavus and Others v Russia* (dec.), nos. 12468/15, 23489/15, 19074/16, ECHR 2020.

50 *Bulgakov v Russia* (dec.), no. 20159/15, ECHR 2020.

51 *Engels v Russia* (dec.), no. 61919/16, ECHR 2020.

52 Dirk Voorhoof, 'ECtHR: Vladimir Kharitonov v Russia, OOO Flavus and Others v Russia, Bulgakov v Russia, Engels v Russia' (2020) 1 IRIS 8.

In the *OOO Flavus* case, the applicants, owners of opposition media outlets, sought judicial review of the blocking measures. OOO Flavus owns grani.ru, the second applicant, Garry Kasparov, is the founder of www.kasparov.ru, and OOO Mediafokus owns the Daily Newspaper (Ezhednevnyy Zhurnal). In March 2014, Roskomnadzor blocked access to their websites at the request of the Prosecutor General, citing the alleged promotion of mass disorder or extremist speech under section 15.3 of the Information Act. This blocking occurred without a court order. The applicants argued against the wholesale blocking of their websites and the lack of specific notice regarding the offending material, which prevented them from taking corrective action to restore access before the Taganskiy District Court and later before the Khamovnicheskiy District Court in Moscow. However, their applications were unsuccessful as both courts rejected the appeal, claiming that 'the blocking measure had had no incidence on the applicants' rights or freedoms'.[53] The applicant appealed the previous domestic decisions before the Moscow City Court which dismissed the appeal in summary fashion, affirming the previous courts' decisions, resulting in the fact that the applicants had exhausted all domestic remedies.

In the *Bulgakov* case, the applicant discovered that the local Internet service provider had blocked access to his website, Worldview of the Russian Civilization (*sic!*), based on a court judgment from April 2012, of which he had been unaware. The judgment, issued under section 10(6) of the Information Act, targeted an electronic book in the files section of the website previously categorised as an extremist publication. The court ordered the block order by instructing the provider to block access to the IP address of the applicant's website. Upon learning of the court's judgment, the applicant promptly removed the e-book. However, the courts declined to lift the blocking measure, citing that the initial court order had directed a block on access to the entire website by its IP address, not solely to the offending material.

Last, per the *Engels* case, a Russian court ordered the local Internet service provider to block access to the applicant's website, RosKomSvoboda, which focused on freedom of expression and privacy issues. This action was based on a complaint filed by a prosecutor, who contended that the information available on the applicant's website regarding bypassing content filters should be banned in Russia. The prosecutor argued that such information enabled users to access extremist material on another unrelated website. Notably, the applicant had not been notified of these legal proceedings. Following the court order, Roskomnadzor requested the applicant to remove the disputed content to prevent the website from being blocked. The applicant complied with this request. However, despite the applicant's argument that providing information about tools and software for browsing privacy protection did not violate any Russian law, the courts rejected his complaint without addressing this central argument.

[53] *OOO Flavus and Others v Russia* § 9.

The reason behind examining the cases together stems from the fact that all the applicants involved in the above cases claimed the violation of Article 10 of the ECHR and the lack of effective remedy (Article 13). Furthermore, in all four cases, the Court was unanimous in finding a violation of Article 10. The ECtHR emphasised the crucial role of the Internet in enabling freedom of expression and information. It found that the measures blocking access to websites constituted an interference with the applicants' rights to impart and receive information. However, these measures failed to meet the conditions required by the Convention, particularly the requirement of being 'prescribed by law'.

In the *Kharitonov* case, the latter's website was blocked under section 15.1 of the Information Act despite not containing any illegal material itself, but solely because it shared the same IP address as a website with illegal content. This lack of legal basis rendered the interference unlawful.

Additionally, in the cases of *OOO Flavus and Others*, the websites were blocked under section 15.3 of the Information Act based on vague grounds, such as calls for mass disorder or participation in unauthorised public events. The notices issued by Roskomnadzor failed to specify particular web pages, preventing the applicants from addressing the specific content in question. Moreover, the Court found no justification for the wholesale blocking of entire websites, which it deemed an extreme measure akin to banning a newspaper or television station. The Government's failure to specify legitimate aims for the blocking measures raised serious concerns, particularly regarding the potential suppression of opposition media.

In Mr. Bulgakov's case, although the e-book on his website was deemed extremist material, he promptly removed it, yet the blocking measure lacked proper legal basis and justification. Moreover, none of the remedies available to the applicants proved effective, leading to a violation of Article 13 in conjunction with Article 10 in each case.

Finally, in the *Engels* case, the ECtHR unanimously found violations of both Article 10 and Article 13 with regard to effective domestic remedies. The Court, in its judgment, highlighted that the existing legal framework on which the decision to block Engels' website was too vaguely formulated. In this regard, the Court underlined that due to the fact that the applicant had been 'coerced' to delete the content in question from the website, Russia had violated Engels' rights under Article 10, noting that this interference not only affected the applicant's right to impart information but conversely, the public's right to receive information as well. As for Article 13 – though domestic remedies were available and duly exhausted by the applicant – the Court accentuated once again that the proceedings lacked safeguards. The Court argued that despite the possibility of appeal, the appellate court had failed to address the substance of the grievance, rendering the remedy ineffective.

5 *Wikimedia Foundation Inc. v Turkey*[54]

In the *Wikimedia Foundation* case, once again, the Turkish regulation on Internet blocking was the focal point. Per the facts of the case, following the Government's request, the Presidency of PIT was instructed to either remove two specific pages from Wikipedia, entitled 'State-Sponsored Terrorism' and 'Foreign involvement in the Syrian Civil War' or alternatively, block the entire website if removal was not feasible.[55] On the same day, the applicant's lawyer received five emails from the PIT demanding the removal of five URL pages within a four-hour timeframe.[56] The PIT decided to block access to the entire website due to the failure to remove the specified pages within the given time limit. It had been deemed technically impractical to block only those specific pages.[57] After the exhaustion of all domestic remedies, the applicant lodged a complaint before the ECtHR.

The Government presented three main arguments against the admissibility of the applicant's complaint. First, it contended that the applicant lacked victim status as the Constitutional Court's ruling recognised the alleged violation, and the subsequent reopening of the case by the domestic court (Criminal Judgeship of Peace of Ankara, CJPA) constituted appropriate redress. Second, it asserted that the applicant had failed to exhaust domestic remedies, highlighting that the individual appeal was pending before the Constitutional Court when the application had been filed to the European Court. Last, the Government urged the Court to declare the application inadmissible due to personal and material incompatibility, suggesting that the Court should focus solely on examining judicial guarantees in the specific case rather than abstract analysis and arguing that the content of the implicated pages fell outside the scope of Article 10 protection under the Convention.[58] The applicant argued that despite the individual appeal route to the Constitutional Court (CC) theoretically providing an effective remedy, it had become ineffective in practice due to systemic issues. She contended that the CC had essentially acted as a first-instance court in examining the legality of such blocking measures, rendering the individual appeal ineffective.

Furthermore, the control exercised by CJPA raised systemic concerns as thousands of websites had been blocked without effective judicial oversight, forcing parties to resort to individual appeals before the CC for unblocking. The applicant asserted that the CC's review process was slow, often delayed until after the case was communicated by the European Court, making it a conditional recourse. Additionally, she claimed that the CC's authority was being disregarded in practice, as evidenced by continued blocking despite CC rulings finding violations in similar cases. Furthermore, the applicant highlighted the inability to

54 *Wikimedia Foundation Inc. v Turkey*, no. 25479/19, ECHR 2022.
55 *Wikimedia Foundation Inc. v Turkey* § 3.
56 *Wikimedia Foundation Inc. v Turkey* § 4.
57 *Wikimedia Foundation Inc. v Turkey* § 5.
58 *Wikimedia Foundation Inc. v Turkey* § 20.

directly challenge legislation, such as Article 8/A of Law No. 5651, before the CC, further complicating the remedy process. Thus, she maintained her victim status, arguing that the CC's failure to address systemic issues left her complaints under Articles 6 and 13 unaddressed.[59]

The Court recalled that it was primarily the responsibility of national authorities to rectify Convention violations. Whether an applicant could still claim victim status depended on the situation at the time of application and on all circumstances, including any developments before the Court's examination. A decision or measure in the applicant's favour typically did not deprive them of victim status unless the authorities explicitly recognised and remedied the Convention violation. In this case, despite the Constitutional Court's finding of violation and subsequent lifting of the contested measure, the applicant contested the Government's arguments, maintaining her victim status due to the alleged systemic issue. Regarding the effectiveness of individual appeals, the Court noted its previous rulings that such appeals should be exhausted, particularly in freedom of expression cases. It found no reason to deviate from this jurisprudence, as there was insufficient evidence to suggest that an individual appeal to the Constitutional Court would not provide adequate redress. The Court observed the Constitutional Court's established jurisprudence on website blocking, noting its criteria for such measures and its previous rulings, finding them disproportionate.

Additionally, it addressed the applicant's argument regarding the inability to challenge legislation directly, highlighting that her challenge to the law's predictability could be raised in an individual appeal. While acknowledging the systemic issue raised by the applicant, the Court found no compelling evidence that the Constitutional Court could not address it. It emphasised the Constitutional Court's ability to establish guiding criteria and the potential for pilot judgment procedures to tackle systemic issues. Despite the lengthy proceedings before the Constitutional Court, the Court did not find the duration manifestly excessive, though it stressed the importance of swift judicial review in such cases. The applicant's complaint under Articles 6 and 13 was considered by the Constitutional Court under the right to freedom of expression, aligning with the Court's jurisprudence, according to which complaints are defined by the facts alleged rather than the legal arguments. Ultimately, the Court concluded that the Constitutional Court's acknowledgement of the violation and its adequate redress meant the applicant had lost victim status. Therefore, the application was deemed incompatible *ratione personae* with the Convention and deemed inadmissible.[60]

[59] *Wikimedia Foundation Inc. v Turkey* §§ 21–26.
[60] *Wikimedia Foundation Inc. v Turkey* §§ 50–51.

6 *Taganrog LRO and Others v Russia*[61]

The case concerned the forced dissolution of Jehovah's Witnesses religious organisations in Russia, the banning of their religious literature and international website on charges of extremism, the revocation of their permit to distribute religious magazines, the criminal prosecution of individual Jehovah's Witnesses (JW), and the confiscation of their property.[62] The jointly handled cases involving the forced dissolution of the local JW organisation, Taganrog, the banning and confiscation of religious publications in different Russian regions, the criminal prosecution of the applicants for distributing 'extremist' literature, the forced dissolution of a local JW organisations (eg Samara) and the JW Administrative centre, the withdrawal of the distribution permit and prosecution of applicants for the distribution of unregistered media and the seizure of a consignment of religious literature and in relation to RATI, the banning of access to the JW's website (jw.org) – in sum, an all-out, total attack on JW as a religion and an organisation. The latter restriction is of utmost importance, especially from a procedural perspective. In 2013, the Tsentralniy District Court in Tver (TDCiD), following an application by a prosecutor, pronounced that the website was 'extremist' as it contained digital brochures and articles concerning the studies and beliefs of the JW community. Per the facts of the case, however, the pertaining applicants, Watchtower Bible and Tract Society of New York (together: WNY), were not informed of the proceeding against them as the TDCiD held that the inclusion and the participation of WNY was unnecessary, given that they were operating an allegedly extremist website.[63] WNY, in an unorthodox manner, was informed of the proceeding via media reporting. Consequently, appeals were filed by WNY and individual JW members, arguing that they were not given a fair chance to participate in the proceedings. The TDCiD initially overturned the decision, citing procedural errors and the absence of extremist materials on the website within Russia. However, the Supreme Court of the Russian Federation reinstated the extremist designation despite objections and logistical issues faced by WNY. Subsequently, in 2015, the Ministry of Justice added 'jw.org' to the Federal List of Extremist Materials, 'cementing' its status as extremist in Russia. The WNY challenged the decision before the ECtHR.

With regard to the alleged violation of Article 10 concerning the banning of the website and deeming it extremist, the applicants highlighted procedural flaws and denial of participation. The Russian government argued that jw.org contained materials previously declared extremist by Russian courts, referencing brochures and magazines deemed as such. It asserted that the website's content posed a threat to public order and safety. Additionally, Russia claimed that the presence of extremist materials justified branding the entire website as extremist, despite the existence of non-extremist religious content and further

[61] *Taganrog LRO and others v Russia*, nos. 32401/10 and 19 others, ECHR 2022.
[62] *Taganrog LRO and others v Russia* § 1.
[63] *Taganrog LRO and others v Russia* § 80.

emphasised their authority to act against materials they deemed as extremist to protect Russian citizens from potentially harmful ideologies.

The ECtHR when assessing the case accentuated once again the pivotal role of the Internet in both freedom of expression and accessing information.[64] The Court also reiterated the findings of the *OOO Flavus* case, marking the dichotomy of information access as a dual right as it entails both the imparting and the receiving/accessing of information. Focusing on Article 10, the Court found that the lack of procedural safeguards in Russian law exacerbated the infringement of rights to impart and access information. The Court criticised the absence of mechanisms allowing website owners to participate in blocking proceedings or remove offensive content before enforcement. Furthermore, the Court underlined that the broad blocking of the entire website, as opposed to the targeted removal of specific allegedly unlawful content, demonstrated disregard for the distinction between legal and illegal information.[65] The Court found that such indiscriminate measures had violated the principles of necessity and proportionality. Subsequently, the Court found that the interference was not prescribed by law and was not necessary in a democratic society.

IV Chasing a Wild Goose? – Drawing Consequences from ECtHR Case Law

Taking into account the above judgments, the following table summarises the decisions on general Internet restrictions in Turkey and Russia.

Table 2: Distribution of judgments in view of violation of Article 10 and admissibility (Source: Own editing)

Country	**Judgment**		
	No violation of Article 10	*Violation of Article 10*	*Inadmissible*
Turkey	0	2	2
Russia	0	5	0
Σ	**0**	**7**	**2**

The evidence per the judgments seems quite clear: Turkey and Russia have a systemic issue with the RATI. Interestingly, however, this systemic problem stems from the first part of the tripartite test,[66] namely, whether the restriction of the RATI was prescribed by law. As

[64] *Ahmet Yıldırım v Turkey* §§ 48–54.

[65] *Taganrog LRO and others v Russia* § 232.

[66] Gehan Gunatilleke, 'Justifying Limitations on the Freedom of Expression' (2020) 22 Human Rights Review 91, DOI: http://dx.doi.org/10.1007/s12142-020-00608-8

seen in all seven cases where violation of Article 10 was decided, questions about legitimacy were raised about the Turkish and Russian legislation. Whether concerning the applicability or the arbitrary enforcement of the respective law, a sequential criticism emerging from the ECtHR case law findings may be examined.[67] The question can rightly be raised: Why do Turkey and Russia not amend their legislation regarding the RATI? Besides being a juridical issue, the legitimacy of the question may be substantiated by the economic factors associated with the above judgments. For instance, in the *Taganrog LRO* case, Russia was ordered to pay around 63.6 million USD in pecuniary and 3.7 million USD in non-pecuniary damages.

Though answers to the question may derive from societal, political or even technical standpoints, following the line of argumentation in the above segments, it can be speculated that from the perspective of a leader of a hybrid regime, the newfound freedom of communication that the Internet has created presents a dilemma as it contradicts the former's inclination to regulate the content and dissemination of information.[68] Kristin Eichhorn and Eric Linhart also stress that Internet restrictions can be a means of hindering the flow and extent of critical views about the respective regime.[69] In this context, I argue that with regard to the websites blocked in Turkey and Russia, such as social media websites and YouTube, the restrictions of the RATI not only constitute a local polemic but a global one – the marginalisation of Turkish and Russian Internet users in an ever-growing and interconnected digital sphere.

Lamentations about the future of the above marginalisation leave no room for optimism. Both scholars and journalists have noted Turkey's systemic Internet and specific website blockings. Between 2014 and 2018, a total of 245,000 websites were banned in Turkey,[70] including the likes of Wikipedia and Facebook, leaving users of these sites two options: to either leave behind these online spheres or use VPNs to access them. Turkey has also recently passed the so-called 'censorship law' on online reporting, criticised by Article-19 and Human Rights Watch, two renowned NGOs specialised in human rights and freedom of expression, for its 'draconian' sanctions for disseminating critical views online, such as criminal penalties and, potentially, prison sentences.[71] Istanbul-based civil society,

---

[67] Gergely Gosztonyi, 'The European Court of Human Rights: Internet access as a means of receiving and imparting information and ideas' (2020) 6 (2) International Comparative Jurisprudence, DOI: http://dx.doi.org/10.13165/j.icj.2020.12.003

[68] Christian Göbel, 'The Information Dilemma: How ICT Strengthen or Weaken Authoritarian Rule' (2013) 115 (4) Statsvetenskaplig Tidskrift 115.

[69] Kristin Eichhorn and Eric Linhart, 'Election-Related Internet-Shutdowns in Autocracies and Hybrid Regimes' (2022) 33 (4) Journal of Elections, Public Opinion and Parties 705, DOI: http://dx.doi.org/10.1080/17457289.2022.2090950

[70] Luke Edwards and Chiara Castro, 'What Websites and Online Services Are Blocked in Turkey – Facebook, Wikipedia and More' (2022) Techradar <https://www.techradar.com/vpn/websites-online-services-blocked-turkey-facebook-wikipedia> accessed 15 October 2024.

[71] Human Rights Watch, 'Turkey: Dangerous, Dystopian New Legal Amendments' (2022) <https://www.hrw.org/news/2022/10/14/turkey-dangerous-dystopian-new-legal-amendments> accessed 15 October 2024.

Alternatif Bilişim Derneği (Alternative Informatics Association) also drew attention to systemic Internet throttling that has been implemented during emergency situations such as major earthquakes when, curiously, access to the most popular social media platforms such as TikTok and Twitter were mysteriously and without any explanation, shut down for 10 hours.[72] Seemingly, nothing seems to be changing either. Deutsche Welle reported that before the local elections, the Turkish government was censoring websites (around 712,000 in 2022 alone) and VPN services, too, leaving absolutely no room for citizens to access information.[73] In this regard, President Erdoğan saying 'We will defeat the opposition in all their strongholds' sustains both the worry and the hopelessness of those who argue that the RATI should be regarded as a human right.[74]

The situation in Russia proves to be even worse; Dasha Litvinova calls the Russian measures regarding the Internet a process of creating a *cyber gulag*, a digital environment where the country tracks, censors and controls its citizens.[75] In this regard, reports also suggest that Russian authorities have taken a systemic approach to blocking access to the Internet: shutting down nearly all VPN programs, limiting messaging apps and restricting access to global news sites and social media sites, such as Instagram.[76] In contrast to Turkey, however, Russian citizens have even less international legal protection. As announced in late 2022, Russia ceased to be a party to the ECHR six months after its exclusion from the Council of Europe.[77] This means that Russian citizens who are not satisfied with the decisions of local courts no longer have any international legal remedies for challenging domestic decisions.

V Conclusions

The persistent violations of Article 10 of the ECHR underscore systemic issues with Turkey and Russia's legislative frameworks. Despite international scrutiny, both governments show little willingness to amend restrictive Internet laws, driven by economic, legal, and political

---

72 EDRI, 'Internet Restrictions in Turkey – European Digital Rights (EDRi)' (2023) <https://edri.org/our-work/internet-restrictions-in-turkey-violate-fundamental-rights/> accessed 15 October 2024.

73 Elmas Topcu, 'Turkey: Internet Censorship before Local Elections' (2024) <https://www.dw.com/en/turkeys-internet-censorship-escalates-before-local-elections/a-68066987> accessed 15 October 2024.

74 Topcu (n 73).

75 Dasha Litvinova, 'The Cyber Gulag: How Russia Tracks, Censors and Controls Its Citizens' (2023) APNews <https://apnews.com/article/russia-crackdown-surveillance-censorship-war-ukraine-internet-dab3663774feb666d6d0025bcd082fba> accessed 15 October 2024.

76 Adam Satariano, Paul Mozur and Aaron Krolik, 'Russia Strengthens Its Internet Controls in Critical Year for Putin' (2024) The New York Times <https://www.nytimes.com/2024/03/15/technology/russia-internet-censors-vladimir-putin.html> accessed 15 October 2024.

77 Thomas Giegerich, 'Struggling for Europe's Soul: The Council of Europe and the European Convention on Human Rights Counter Russia's Aggression against Ukraine' (2022) 25 (3) Zeitschrift für Europarechtliche Studien, DOI: https://doi.org/10.5771/1435-439x-2022-3-519

factors. These restrictions extend beyond borders, stifling global discourse and connectivity while marginalising Internet users and suppressing dissent. With escalating measures and diminishing legal protections, the future of digital rights in Turkey and Russia appears grim. Citizens face heightened surveillance and censorship, necessitating advocacy, solidarity and international intervention. Civil society, human rights organisations and the global community must support Internet users in both countries, affirming the right to access the Internet as vital for democracy, freedom of expression and global connectivity in the digital era. The present paper aimed to analyse ECtHR case law, draw conclusions about the future of the RATI in two hybrid regimes and add to the scholarly literature on freedom of expression in autocracies.

Grace X. Yang*

World Internet Conference and China's Promotion of Cyber Sovereignty

Abstract

Despite ongoing criticism, the Chinese government has continuously hosted the World Internet Conference for the last decade. This research explores the motives behind China's persistent efforts, particularly focusing on its strategies for advocating cyber sovereignty. It uses natural language processing and discourse analysis to analyse official documents and Chinese media reports about the World Internet Conference. It finds that China uses discourses aligned with the ideologies of Non-aligned Movement members to facilitate the promotion of cyber sovereignty and leverage the World Internet Conference to build partnerships to influence the development of global cyber governance.

Keywords: World Internet Conference; cyber sovereignty; China; Non-alignment Movement; Natural Language Processing

I Introduction

The World Internet Conference (WIC) is a worldwide annual Internet event jointly hosted in Wuzhen by the Cyberspace Administration of China (CAC) and the Zhejiang Government. It is currently the largest and highest-level Internet Conference in China and one of the largest Internet events in the world. Unlike the multi-stakeholder Internet forum the Internet Governance Forum (IGF), which is accessible to stakeholders around the globe, the WIC is invitation-only; only a few hand-picked businesses and officials are invited.

It has been evident since its inception that WIC is not a simple technical conference but that it has obvious political and diplomatic overtones since each year, top-level Chinese Communist Party (CPC) officials attend, and Chinese President Xi Jinping delivers an opening remark through a letter, video or personal presence. However, it has been *de facto*

* Grace X. Yang, PhD Candidate, Osteuropa Institut, Freie Universität Berlin. This paper was supported by the project 'PRIN 2022KTTSBC – Digital Sovereignty', funded by the Italian Ministry of Research and University. ORCID iD: 0009-0003-9275-4650.

boycotted by major Western countries, especially the United States (US) and criticised as 'a propaganda effort' aimed at promoting the Chinese multilateral model of Internet governance.[1] Yet it has consistently been held for the last decade, since 2014. Why does China insist on hosting the event, and what message is China trying to convey through it?

II Literature Review

Unlike almost all other countries, since it was connected to the World Wide Web in the early 1990s, the Chinese government has controlled all online access routes. The Great Firewall (the Golden Shield Project) was built shortly after this,[2] and national sovereignty has 'naturally' been extended to cyberspace. As stated in the widely cited White Paper on the Internet in China issued by the Information Office of the State Council of China in 2010, the Internet has been regarded as a component of China's infrastructure. Further, the Internet within Chinese borders comes under PRC sovereignty and jurisdiction, and the state plays the leading role in its administration.[3]

In the context of the Arab Spring and visions of what may occur when the Internet is not under state control, China proposed a code of conduct for state behaviour that aims to identify the rights and responsibilities of states in relation to cyber governance at the UN General Assembly together with Russia and other Shanghai Cooperation Organization members in 2011 and 2015. The proposals called for a re-evaluation of the then cyber governance model and emphasised the key role of states in managing domestic cyber affairs. Sovereignty was proposed as the first principle of cooperation in cyberspace at the Budapest Conference on Cyberspace in 2012 by the Chinese delegation, entitling every state to 'formulate its policies and laws in light of its history, traditions, culture, language and customs'.[4]

Edward Snowden's revelations about the US National Security Agency's global espionage campaigns in 2013 stimulated the proliferation of Chinese academic literature on Internet sovereignty, with a focus on how to defend the cyber border. In 2014, the first WIC in Wuzhen was held, and Chinese President Xi Jinping put forward the term

---

1 Milton Mueller, 'Wuzhen Promotes the Chinese Internet Way (with a Little Help from Its Friends)' (30 November 2016) Internet Governance Project, <https://www.internetgovernance.org/2016/11/29/wuzhen-promotes-the-chinese-internet-way-with-a-little-help-from-its-friends/> accessed 15 October 2024.

2 Gergely Gosztonyi, 'Special models of internet and content regulation in China and Russia' (2021) (2) ELTE Law Journal 92, DOI: https://doi.org/10.54148/ELTELJ.2021.2.87

3 Information Office of the State Council of the People's Republic of China, 'The Internet in China' (2010) <https://nsarchive.gwu.edu/document/20842-03> accessed 15 October 2024.

4 Huikang Huang, 'Statement by Huang Huikang, Director General of the Department of Treaty and Law of the Ministry of Foreign Affairs, at the Budapest International Conference on Cyber Issues' Ministry of Foreign Affairs of the People's Republic of China, 4 October 2012 <https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/tyfls_674667/xwlb_674669/201210/t20121009_7669976.shtml> accessed 15 October 2024.

'Internet sovereignty' publicly for the first time. At the second WIC, he further claimed that 'we should… respect Internet sovereignty… respect the right of individual countries to independently choose their path of cyber development and model of cyber regulation and participate in international cyberspace governance on an equal footing.'[5]

Since then, the idea of 'Internet sovereignty' has been mentioned frequently by the top leaders of the CCP, including the former Internet 'Czar' Luwei and has been included in discourses and policies by Chinese officials, media and scholars. It has been considered a milestone for China in terms of the definition of norms in the field of global Internet governance. Fang Binxing, the so-called 'Father of China's Great Fire Wall', emphasised the 'man-made' nature of cyberspace, the instrumental aspect of data and the need for the equal participation of sovereign countries in global cyberspace governance in his book Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace in 2019. Four versions of the White Paper, Sovereignty in Cyberspace: Theories and Practices were unveiled at the World Internet Conference since 2019, which define the concept, fundamental principles and related practices, thus may be taken as the latest effort of the Chinese government to formulate the respective norms.

China advocates a state-centred and bordered Internet, which is based on territorial sovereignty, focusing on individual responsibilities, maximising economic benefits and minimising political risks for the sake of the one-party rule,[6] while the US and other major Western countries advocate an individual-based, rights-centred, market-driven, single and connected Internet. This became especially relevant when, in 2011, China overtook the US as the global leader in terms of the installation of telecommunication bandwidth. By 2014, its bandwidth was double that of the US.[7] Contestation in the global cyber governance arena between China and the West, especially the US, has been deeply rooted since the beginning of the Internet epoch.

However, due to the Chinese policy formulation process, Zeng and others find – by unpacking the Chinese discourse about 'Internet sovereignty' by analysing Chinese-language literature – that the disagreements and uncertainty within China over its meaning and measures for putting it into practice are huge.[8] For example, there is unresolved

---

5 Jinping Xi, 'Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference' Ministry of Foreign Affairs of the People's Republic of China, 16 December 2015 <https://chinacopyrightandmedia.wordpress.com/2015/12/16/speech-at-the-2nd-world-internet-conference-opening-ceremony/> accessed 15 October 2024.

6 Min Jiang, 'Authoritarian Informationalism: China's Approach to Internet Sovereignty' (2010) 30 (2) SAIS Review of International Affairs 73, DOI: https://doi.org/10.1353/sais.2010.0006

7 David Robson, 'Why China's Internet Use Has Overtaken the West' (9 March 2017) BBC, <https://www.bbc.com/future/article/20170309-why-chinas-internet-reveals-where-were-headed-ourselves> accessed 15 October 2024.

8 Jinghan Zeng, Tim Stevens, Yaru Chen, 'China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"' (2017) 45 (3) Politics & Policy 432, DOI: https://doi.org/10.1111/polp.12202

discussion about the relative merits of the terms 'information sovereignty', 'Internet sovereignty', and 'cyber sovereignty', the scope of which concepts are broadening; there are also disagreements about the origins of the term (whether it derives from China alone, or it has other origins, such as the NATO-sponsored Tallinn Manual); there are also debates around the concept of 'network frontiers', ie how to define the limit of the application of sovereignty. Although China has a great interest in promoting China's normative position in global cyber governance, the fragmented and underdeveloped domestic formulation of the discourse has restricted the process.

Roger Creemers argues that China's notion of 'cyber sovereignty' involves three normative dimensions that starkly contrast with traditional cyber governance. First, the idea that national governments possess sovereign rights to regulate all online activities within their borders directly conflicts with the global connectivity and openness of the Internet. Second, the assertion of national sovereignty over non-state actors contradicts the multi-stakeholder model promoted by Western countries. Third, the principle that all sovereign states are equal poses a direct challenge to the longstanding dominance of the US in cyberspace.[9]

According to Sarah McKune and Shazeda Ahmed, China's understanding of 'Internet sovereignty' has three dimensions: 'Internet governance', 'national defence', and 'internal influence.'[10] Segal argues that Xi's cyber diplomacy has three major aims. The first is to limit the threat posed by the Internet and the flow of information to the domestic stability and legitimacy of the regime; the second is to extend China's influence in the military, political and economic spheres; the third is to counter the US's advantage and increase China's room for manoeuvre. China is pursuing a 'parallel track' of managing state-to-state relations while trying to generate international norms which could improve its domestic control of the flow of information.[11]

Andrew Devine posits that China assumes four distinct roles within the WIC: developer, global leader, global village member and law-abiding citizen. According to Devine, China strategically adopts these roles to persuade developing and emerging countries to embrace its preferred governance model, cyber sovereignty. The countries targeted are those where China wields economic influence as a developer or political influence as a global leader, particularly in areas where the US has scaled back its involvement in foreign affairs.[12]

---

[9] Rogier Creemers, 'China's Conception of Cyber Sovereignty: Rhetoric and Realization' in DWJ Broeders, van den. B. B. (eds), *Governing cyberspace: Behavior, power and diplomacy* (Rowman and Littlefield 2020, London) 114–115, DOI: https://doi.org/10.2139/ssrn.3532421

[10] Sarah Mckune, Shazeda Ahmed, 'The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda' (2018) 12 International Journal of Communication 3835.

[11] Adam Segal, *Chinese Cyber Diplomacy in a New Era of Uncertainty* (2 June 2017) Hoover Institution <https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf> accessed 15 October 2024.

[12] Andrew Devine, 'Contesting the Digital World Order' (2019) 42 Politikon 61, DOI: https://doi.org/10.22151/politikon.42.3

States that support the concept of cyber sovereignty often do so thinking that the status quo favours a US-favoured, techno-imperialist regime at odds with democratic decision-making, which 'allows the US to enforce rather easily its domestic policies, at times with extraterritorial effects'.[13] Therefore, the phenomenon of cyber sovereignty may serve to establish cyber territoriality within a country's borders and diminish the hegemonic power of the Western-led liberal order.

Mueller argues that China is trying to incentivise other developing countries to internalise and adapt its model of realigning control of communication with the jurisdictional boundaries of national states through the WIC.[14] McKune and Ahmed argue that the World Internet Conference's fundamental goal is to combine forces with developing countries to gain international respect for the idea of Internet sovereignty and authoritarian digital practices.[15] Karmazin points out that China is organising this conference to promote its views globally and mobilise potential allies.[16]

III Theory and Hypothesis

The paper's entry point is the idea of a 'norm', which is mainly adopted from the theory of social constructivism. Unlike neo-realism, which focuses on material capabilities and the distribution of power, social constructivism emphasises the role of ideas, identities and social practices. The identities and interests of states are not given but formed through social interaction.[17] The mutual constitution of social structure and agency is the foundation of social constructivism, with norms serving as the link between these two elements. Social constructivism stresses that ideas and communicative processes primarily determine which material factors are deemed relevant and shape the understanding of interests, preferences and political decisions.[18]

---

13 Richard Hill, 'Chapter 4 Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means?' in Roxana Radu, Jean-Marie Chenou, Rolf H Weber (eds), *The Evolution of Global Internet Governance: Principles and Policies in the Making* (Springer 2014, Cham) 86, DOI: https://doi.org/10.1007/978-3-642-45299-4_5

14 Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Wiley 2017, New Jersey).

15 Mckune, Ahmed (n 10) 3845.

16 Aleš Karmazin, 'China's Promotion of Cyber Sovereignty Beyond the West' in Šárka Kolmašová, Ricardo Reboredo (eds), *Norm Diffusion Beyond the West: Agents and Sources of Leverage* (Springer 2023, Cham) 61, DOI: https://doi.org/10.1007/978-3-031-25009-5_4

17 Alexander Wendt, 'Anarchy Is What States Make of It: The Social Construction of Power Politics' (1992) 46 (2) International Organization 394, DOI: https://doi.org/10.1017/S0020818300027764

18 Martha Finnemore, Kathryn Sikkink, 'Taking Stock: The Constructivist Research Program in International Relations and Comparative Politics' (2001) 4 Annual Review of Political Science 393, DOI: https://doi.org/10.1146/annurev.polisci.4.1.391

According to Fennimore and Sikkink, there are three stages in the 'life cycle' of a norm.[19] The first stage is called 'norm emergence', a process of persuasion by 'norm entrepreneurs'; the second is called the 'norm cascade', involving norm acceptance, which is characterised by imitation of the norm by followers of the norm entrepreneurs; the third is the internalisation of a norm, referring to when norms have acquired a taken-for-granted quality and are no longer a topic of public debate. There is a 'tipping point' after the second stage when the norm has been adopted by a critical proportion of relevant state actors. Many norms do not reach this tipping point, so the completion of the life cycle is not inevitable.

For the emergence of a norm, the existence of a norm entrepreneur and 'organisational platforms' are essential.[20] Norm entrepreneurs use language to name, interpret and dramatise norms in a usually contested environment where alternative norms exist. Norm diffusion occurs through social interaction, and norms which are aligned with the target audience's existing beliefs and practices may facilitate diffusion. Organisational platforms at an international level are used by norm entrepreneurs to promote their norms. The norms must be institutionalised in some international rules or organisations for them to reach the second stage. After the tipping point, more countries may adopt the norms without domestic pressure to change. After internalising specific norms, the state's identities and interests may conform accordingly.

Based on this theory, the author formulates the following hypothesis: China tries to promote cyber sovereignty through WIC with discourses acceptable to the targeted audiences and leverages the WIC to build strategic partnerships and alliances to promote cyber sovereignty, particularly with countries sceptical of the Western model.

IV Data and Methodology

The primary data sources for this research are the official documents associated with the World Internet Conference (some manually translated from Chinese to English), and Chinese news media coverage retrieved from the database Lexisnexis Uni in the period from 1 January 2014 to 1 August 2023.

Among the overwhelming Chinese media coverage of WIC, China Daily appears to be the media outlet that has covered this event most comprehensively and in-depth over the years. It is the leading English-language newspaper, telling Chinese stories to the world. It covers all continents globally, reaching a total readership of more than 350 million, and is the most quoted Chinese publication by foreign media.[21] China Daily has different editions

[19] Martha Finnemore, Kathryn Sikkink, 'International Norm Dynamics and Political Change' (1998) 52 (4) International Organization 895, DOI: https://doi.org/10.1162/002081898550789

[20] Finnemore, Sikkink (n 19) 897.

[21] 'About China Daily Group' China Daily <https://www.chinadaily.com.cn/e/static_e/about#> accessed 15 October 2024.

for different regions, including North and South America, Europe, the Asia-Pacific and Africa. The 'global edition' coverage was selected for this research because other editions generally repeat this version. Altogether, 906 reports mentioning WIC were collected during the period under analysis for this research.

Natural language processing (NLP) with Python was used to analyse official documents and media coverage. NLP is at the intersection of computer science and linguistics and began in the 1950s;[22] it is a method to extract meaningful information from large quantities of text data with the help of machine learning. In this research, frequent analysis is used to identify the most frequently occurring terms, sentiment analysis is used to evaluate the sentiment of the news reports, and temporal analysis is used to trace the frequency of words over time.

V Finding and Discussions

The themes of the conferences over the last ten years – as shown in Table 1 – are quite consistent.

Table 1: Themes of World Internet Conferences (Source: Own editing)

2014	An Interconnected World Shared and Governed by All – Building a Cyberspace Community of Shared Destiny
2015	An Interconnected World Shared and Governed by All – Building a Cyberspace Community of Shared Destiny
2016	Innovation-driven Internet Development for the Benefit of All – Building a Community of Common Future in Cyberspace
2017	Developing Digital Economy for Openness and Shared Benefits
2018	Creating a Digital World of Mutual Trust and Collective Governance
2019	Intelligent Interconnection for Openness and Cooperation – Building a Community with a Shared Future in Cyberspace
2020	Digital Empowerment for a Better Future: Building a Community with a Shared Future in Cyberspace
2021	Towards a New Era of Digital Civilization – Building a Community with a Shared Future in Cyberspace
2022	Building a Networked World Together to Create a Digital Future – to Jointly Build a Shared Community in Cyberspace
2023	Creating an Inclusive and Resilient Digital World Benefitting to All

[22] Prakash M Nadkarni, Lucila Ohno-Machado, Wendy W Chapman, 'Natural Language Processing: An Introduction' (2011) 18 (5) Journal of the American Medical Informatics Association 544, DOI: https://doi.org/10.1136/amiajnl-2011-000464

The meaning of this recurring theme is hard to comprehend at first glance, but like many other Chinese foreign policy concepts, it starts as more of a slogan at the beginning and is gradually discussed and defined in Chinese official discourse.[23] In this context, the meaning of 'Building a Community of Shared Future for Mankind in Cyberspace' was defined as the 'Four Principles' (respect for cyber sovereignty, maintenance of peace and security, promotion of openness and cooperation, cultivation of good order) and the 'Five Proposals' (speed up the building of global Internet infrastructure and promote inter-connectivity; build an online platform for cultural exchange and mutual learning; promote the innovative development of a cyber economy for common prosperity; maintain cyber security and promote orderly development; build an Internet governance system to promote equity and justice) by the Chinese President Xi Jinping in his opening remark at the second WIC.[24] These have been abbreviated as the 'Four Principles' and 'Five Proposals' since then.

The Four Principles are believed to be intentionally used to invoke China's 'Five Principles of Peaceful Coexistence' (respect of sovereignty and territorial integrity, nonaggression, non-intervention, equality and mutual benefits, and peaceful coexistence),[25] which were proposed by China when it tried to establish diplomatic relations with neighbouring countries like India and Burma in the 1950s after the establishment of the new country. The five principles were later developed further by the Asian-African Conference (the 'Bandung Conference') convened in Bandung in Indonesia in 1955 into ten principles (the 'Bandung Spirit') to deal with international relations, including respect for the principles of the Charter of the United Nations, respect for sovereignty and integrity, the equality of all races and all nations, non-interference, the right of self-defence, non-aggression, the peaceful settlement of international disputes, mutual interests and cooperation. The Bandung Conference was the starting point for the Non-Aligned Movement (NAM). The concept of nonalignment emerged from the wave of decolonisation after WWII, especially after the Cold War began and when newly independent countries called on each other not to ally with either of the two superpowers but to join forces to support each other's national self-determination against all forms of colonialism and imperialism. The initial leaders of the NAM were India, Indonesia, Yugoslavia, Egypt, Ghana, etc., and there are now 120 member states.[26] Even now, it is still characterised by its vocal opposition to the 'sins of the West'.[27]

---

[23] Jinghan Zeng, *Slogan Politics: Understanding Chinese Foreign Policy Concepts* (Palgrave McMillan Singapore 2020, Singapore) 2.

[24] Xi (n 5).

[25] Karmazin (n 16) 64.

[26] André Munro, 'Non-Aligned Movement (NAM) – Definition, Mission, & Facts | Britannica' (21 June 2024) Encyclopedia Britannica <https://www.britannica.com/topic/Non-Aligned-Movement> accessed 15 October 2024.

[27] Andrew Cheatham, *The New Nonaligned Movement Is Having a Moment* (4 May 2023) United States Institute of Peace <https://www.usip.org/publications/2023/05/new-nonaligned-movement-having-moment> accessed 15 October 2024.

The Five Principles of Peaceful Coexistence have been used to spur cooperation among non-Western countries while portraying China as a leader of these countries. Xi framed cyber sovereignty using a similar discourse in a speech from 2015:

> The principle of sovereign equality enshrined in the *Charter of the United Nations* is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, including cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security.[28]

Since the first conference, a forum called 'International Rules of Cyberspace: Practice and Exploration' has been dedicated to discussing the rule-making of global cyber governance. Guests and keynote speakers are targeted and invited. The three versions of the White Paper on Sovereignty in Cyberspace: Theory and Practice are the results of these discussions. In the first edition of the White Paper in 2019, cyberspace sovereignty was defined as 'the extension of national sovereignty to cyberspace… regarding cyber entities, behavior, infrastructure, information and governance in its territory'.[29] The second edition added an obligation dimension, which includes non-infringement on other countries' interests, non-interference in other countries' internal affairs, due diligence and protection.[30] The 'international law attributes of cyber sovereignty' were added to the third edition. This states that different countries may have different definitions and understandings of the concept of cyber sovereignty, but this does not affect the legal status of cyber sovereignty as an independent principle and rule. From the development process, we can see a clear tendency to define cyber sovereignty as a legal principle with the potential for universal application rather than as a political slogan in Chinese official documents.

What is the main agenda in the WIC's official documents, and how is WIC framed in Chinese media reportage? Frequency analysis of the official documents of the WIC and Chinese media reportage reveals that the top 80 words are the following:

---

28 Xi (n 5).

29 China Institute of Contemporary International Relations, Shanghai Academy of Social Sciences and Wuhan University, 'Sovereignty in Cyberspace: Theory and Practice (Version 1.0)' (21 October 2019) <https://www.wicinternet.org/2019-10/21/c_815434.htm> accessed 15 October 2024.

30 Wuhan University, China Institute of Contemporary International Relations and Shanghai Academy of Social Sciences, 'Sovereignty in Cyberspace: Theory and Practice (Version 2.0)' (26 November 2020) <https://www.wicinternet.org/2020-11/26/c_808744.htm> accessed 15 October 2024.

Table 2: Frequency Analysis of WIC Official Documents and China Daily Reports on WIC (Source: Own editing)

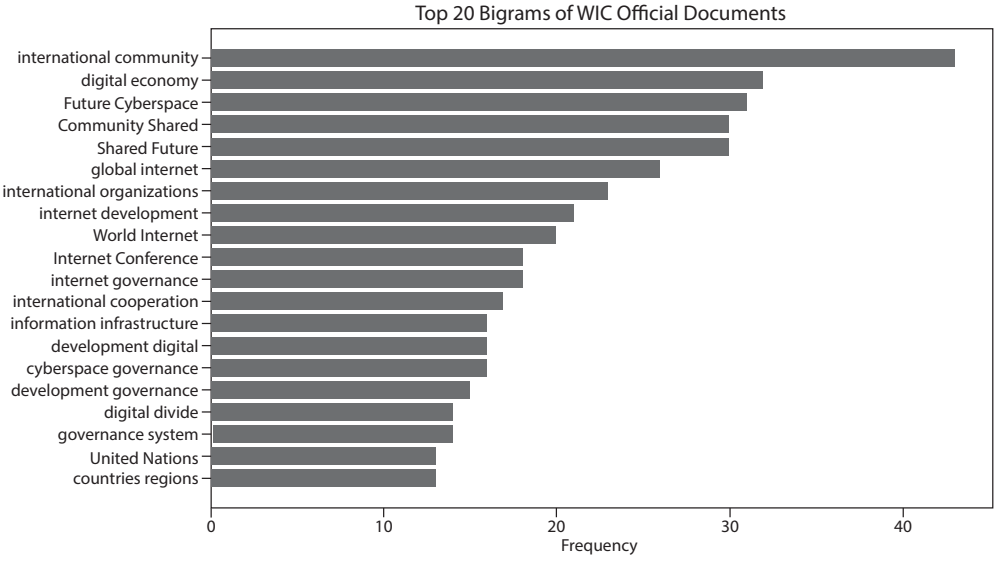
Frequency Analysis of WIC Official Documents (1 January, 2014-1 August 2023)	Frequency Analysis of China Daily Reports on WIC (1 January, 2014-1 August 2023)
	
[('internet', 160), ('development', 157), ('international', 132), ('cyberspace', 132), ('digital', 107), ('global', 95), ('governance', 92), ('countries', 79), ('community', 78), ('new', 74), ('network', 72), ('security', 68), ('cooperation', 64), ('information', 61), ('promote', 52), ('technology', 51), ('economy', 48), ('future', 45), ('cultural', 44), ('organizations', 42), ('Internet', 42), ('promoting', 41), ('infrastructure', 35), ('construction', 33), ('online', 33), ('shared', 32), ('world', 31), ('common', 30), ('data', 30), ('economic', 29), ('World', 28), ('cyber', 28), ('innovation', 25), ('actively', 25), ('human', 24), ('social', 24), ('rules', 24), ('protection', 24), ('mutual', 24), ('cybersecurity', 24), ('become', 23), ('build', 23), ('people', 23), ('system', 23), ('sharing', 23), ('humanity', 22), ('increasingly', 22), ('UN', 22), ('culture', 22), ('challenges', 21), ('together', 21), ('exchange', 20), ('jointly', 20), ('parties', 20), ('exchanges', 20), ('services', 20), ('Conference', 19), ('technical', 19), ('technologies', 19), ('communication', 19), ('regions', 17), ('communities', 17), ('various', 17), ('trust', 17), ('open', 17), ('role', 17), ('becoming', 17), ('Wuzhen', 16), ('national', 16), ('enhance', 16), ('building', 16), ('including', 16), ('important', 16), ('public', 16), ('divide', 15), ('developing', 15), ('integration', 15), ('order', 15), ('companies', 15), ('mechanisms', 15)]	[('internet', 7752), ('china', 6639), ('world', 3518), ('said', 3368), ('conference', 2634), ('wuzhen', 2518), ('development', 2218), ('zhejiang', 1744), ('province', 1631), ('chinese', 1622), ('technology', 1462), ('new', 1434), ('cyberspace', 1425), ('also', 1406), ('digital', 1320), ('international', 1266), ('countries', 1252), ('global', 1250), ('http', 1222), ('people', 1147), ('online', 1021), ('cooperation', 1020), ('year', 1018), ('economy', 995), ('industry', 992), ('daily', 978), ('words', 963), ('information', 957), ('body', 944), ('security', 931), ('length', 913), ('2015', 881), ('companies', 852), ('country', 833), ('xi', 829), ('future', 803), ('data', 768), ('president', 764), ('company', 761), ('governance', 750), ('percent', 739), ('innovation', 733), ('technologies', 722), ('one', 703), ('million', 702), ('market', 687), ('first', 679), ('business', 674), ('years', 668), ('services', 646), ('town', 642), ('economic', 642), ('according', 625), ('east', 622), ('government', 610), ('group', 606), ('ai', 594), ('community', 587), ('second', 579), ('billion', 574), ('platform', 559), ('byline', 556), ('mobile', 553), ('big', 552), ('become', 542), ('including', 541), ('shared', 518), ('users', 514), ('media', 514), ('growth', 511), ('yuan', 503), ('ceo', 500), ('november', 491), ('system', 490), ('dec', 490), ('us', 489), ('december', 489), ('alibaba', 488), ('2016', 483), ('building', 481)]

In the official documents of the WIC, words like 'countries', 'international', 'UN', 'cooperation', 'world' and 'governance' all related to the state, implying international

cooperation and collaboration among different countries, possibly under the auspices of United Nations, are associated with the advocacy of cyber sovereignty and multilateral model of cyber governance.

We identified that some aspects of the Internet are highlighted in the keywords: cybersecurity is underscored by keywords such as 'security', 'protection', 'cybersecurity'; the economic implications and technological development of the Internet are highlighted by 'economy', 'economic', 'innovation', 'companies', 'digital', 'technology'; the physical and technical infrastructure of the Internet is highlighted by 'infrastructure', 'construction', 'build', 'building'; and the social and cultural dimensions of Internet development are underscored by such words as 'community', 'cultural', 'human', 'social', 'humanity' and 'culture'. Meanwhile, 'challenges', 'future', and 'increasingly' are strongly forward-looking words, and 'governance', 'rules', 'exchange' and 'sharing' indicate a state of dissatisfaction with the status quo, pointing to discussions about changes in global cyber governance rules.

To get a better idea of the topics in the official documents, N-gram analyses were conducted, and the top 20 bigrams and trigrams are shown above. Multilateral model advocacy may be seen from keywords such as 'international cooperation', 'United Nations', 'countries regions', 'international governance cyberspace' and 'governments international organizations'. The words 'internet development', 'information infrastructure', 'development digital', 'development governance', 'development digital economy' and 'internet development governance' show a strong development orientation. In contrast, 'shared community' is a recurring theme that shows that advocacy is aimed at developing countries.



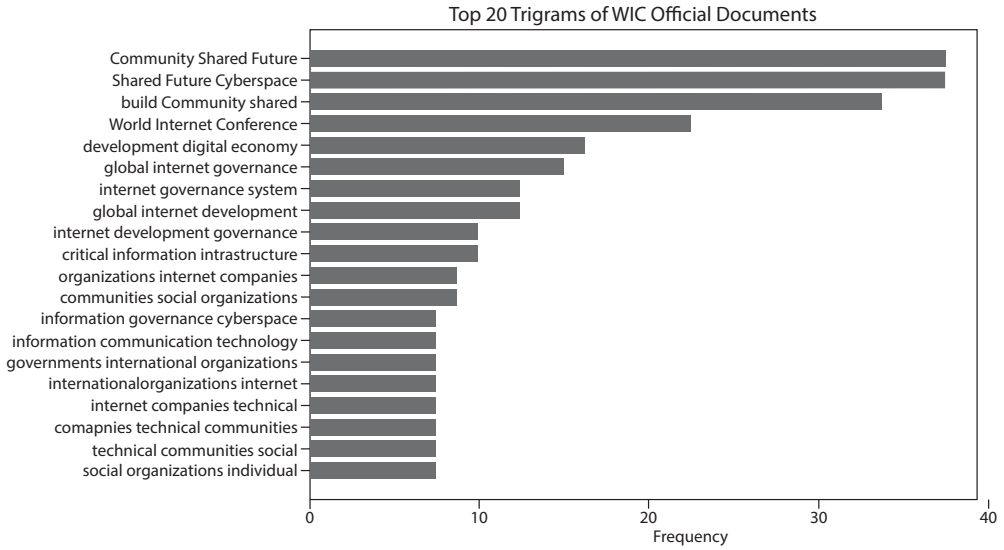


Figure 1: Top 20 Bigrams and Trigrams of WIC Official Documents (Source: Own editing)

From the frequency of words, we can observe the significant themes in Chinese media:

1. A focus on global and international perspectives: Words like 'world', 'international', 'countries' and 'global' indicate that the Chinese media portrays the conference as a global event; 'cooperation' also stands out, highlighting China's intention to collaborate internationally in the digital space; 'Governance' and 'security' suggest discussions around the rules, regulations and security in cyberspace.
2. A focus on technological and economic developments: Words like 'internet', 'technology', 'digital', 'cyberspace', 'data' and 'AI' indicate a strong focus on the conference's technological aspects; the frequent occurrence of 'innovation', 'development', 'economy', 'industry', 'market', 'business' and 'growth' suggests an emphasis on progress and advancements, pointing to the economic importance of digital technologies.
3. Stress on the importance of location: 'Wuzhen' and 'Zhejiang.' Wuzhen is a small town close to Alibaba's headquarters. This e-commerce platform has created enormous opportunities for ordinary people across China to create their own businesses at little cost. Compared to the more elitist and costly 'Silicon Valley' model, Wuzhen is more attractive to developing countries in terms of bridging the digital divide and progressing in digital development.[31]

[31] Anbin Shi, 'China's Role in Remapping Global Communication' in Daya Kishan Thussu, Hugo de Burgh, Anbin Shi (eds), *China's Media Go Global* (Routledge 2017, London) 46, DOI: https://doi.org/10.4324/9781315619668-3

> To obtain a better understanding of the value orientation of the Chinese reports, further analysis of the 'special words' which clearly demonstrate value orientations was conducted on the China Daily reports, and the result is as follows: {'sovereignty': 179, 'multilateralism': 16, 'multistakeholder': 0, 'censorship': 3, 'freedom': 67, 'right': 140, 'human right': 0, 'state': 228, 'government': 610, 'control': 123, 'democracy': 15, 'territory': 8, 'technology': 1462, 'security': 931}

The high frequency of 'sovereignty' (179) and 'government' (610) indicate a strong emphasis on national sovereignty in the context of the Internet, aligning with China's stance on cyberspace sovereignty; China's focus on 'multilateralism' (16) aligns with its preference for state-led Internet governance, while the absence of 'multistakeholder' (0) reflects no interest in involving multiple stakeholders; the high frequency of 'technology' (1462) and 'security' (931) underscores the focus on technological advancement and cybersecurity in the narrative; the low frequency of 'freedom' (67), 'democracy' (15), and 'censorship' (3) indicates limited discussion or avoidance of the topics.

Based on the above discussion, one may wonder who is actually invited to these conferences and who the 'community' China is trying to address is. Due to China's emphasis on the role of states and governments in cyber governance, we focus on governmental representatives only in this research. While the complete participant lists of the conferences over ten years have not been published, we have obtained lists based on the official websites and media reports, although these are not exhaustive.

We find the consistent participation in WIC of the following governments/countries: Afghanistan, Algeria, Argentina, Azerbaijan, Bangladesh, Barbados, Bahrain, Belarus, Burundi, Cambodia, Chile, Colombia, Costa Rica, Cuba, Congo (DRC), Egypt, Equatorial Guinea, Ethiopia, Guinea, Guinea-Bissau, Iran, Iraq, Jordan, Kazakhstan, Kenya, Kiribati, Kyrgyzstan, Laos, Lebanon, Lesotho, Malawi, Malaysia, Maldives, Mauritius, Mexico, Micronesia, Montenegro, Myanmar, Namibia, Nauru, Nepal, Niger, Nigeria, Pakistan, Palestine, Rwanda, Russia, Samoa, Saudi Arabia, Singapore, Somalia, South Korea, Sri Lanka, Sudan, Switzerland, Syria, Tajikistan, Tanzania, Thailand, Turkmenistan, Tuvalu, Uganda, Uzbekistan, Yemen, Zambia, Zimbabwe, etc.

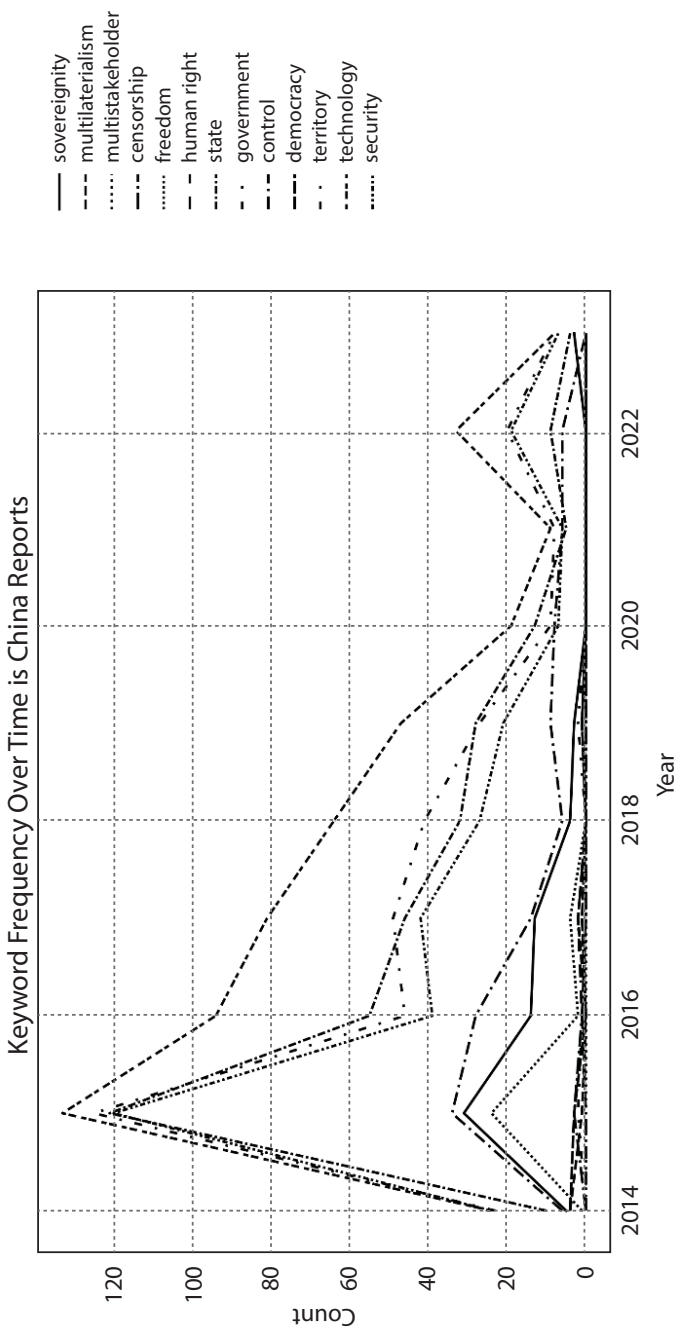


Figure 2: Word Frequency Over Time in China Reports (Source: Own editing)

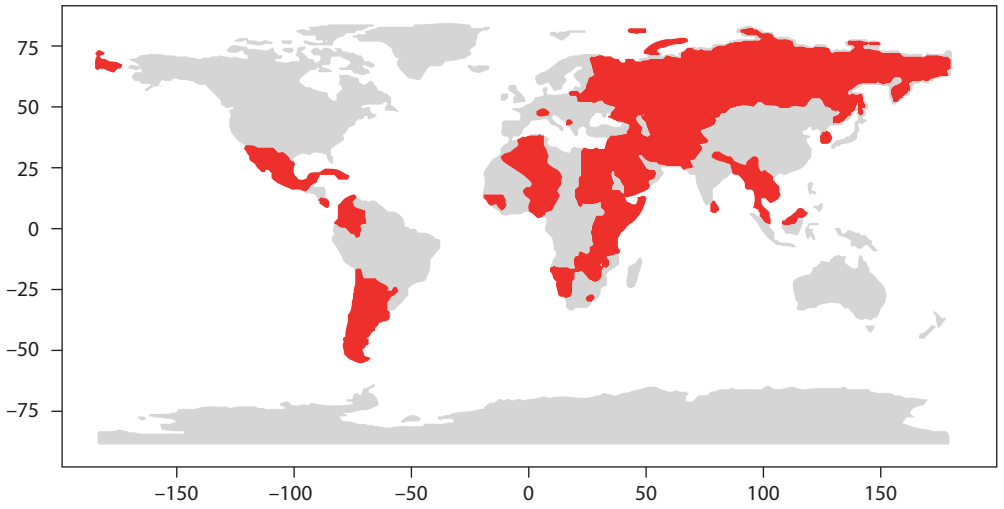


Figure 3: Regular Governmental Participants of the WIC (Source: Own editing)

Most of them are also members of the NAM, which shares the ideology of the Bandung Spirit.

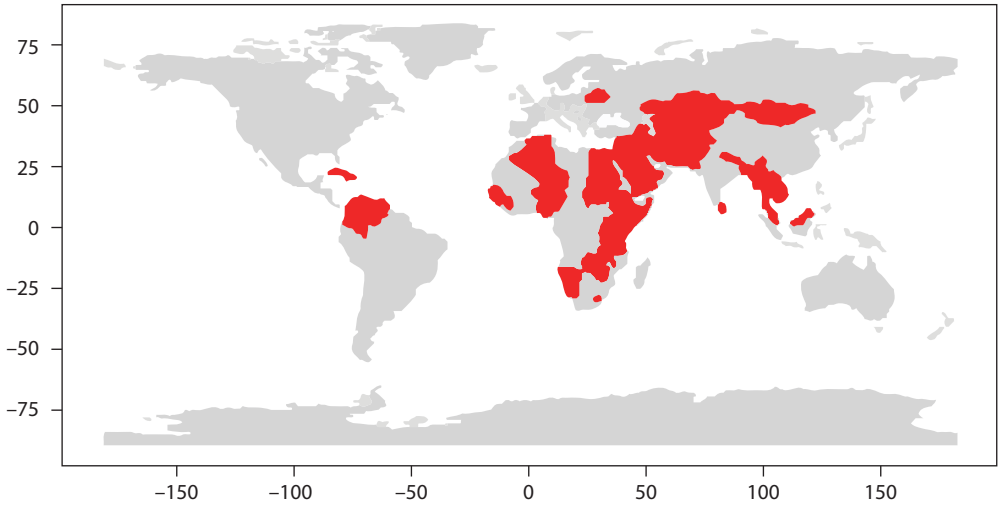


Figure 4: NAM Countries among Regular Governmental Participants of the WIC (Source: Own editing)

Most participating governments are also engaged in China's Belt and Road Initiative (BRI), of which 23 countries are classified as Least Developing Countries, and most are African. In 2021, China launched a 'China-Africa Initiative to Work Together to Build a Community with a Shared Future in Cyberspace' initiative at the China-Africa Internet Development and Cooperation Forum held via video link during the COVID-19 pandemic. In the said initiative, China advocated respect for cyber sovereignty as the premise for expanding Internet access and connectivity to African countries and advocated a leading role for the UN as the primary means of international cyberspace governance.[32]

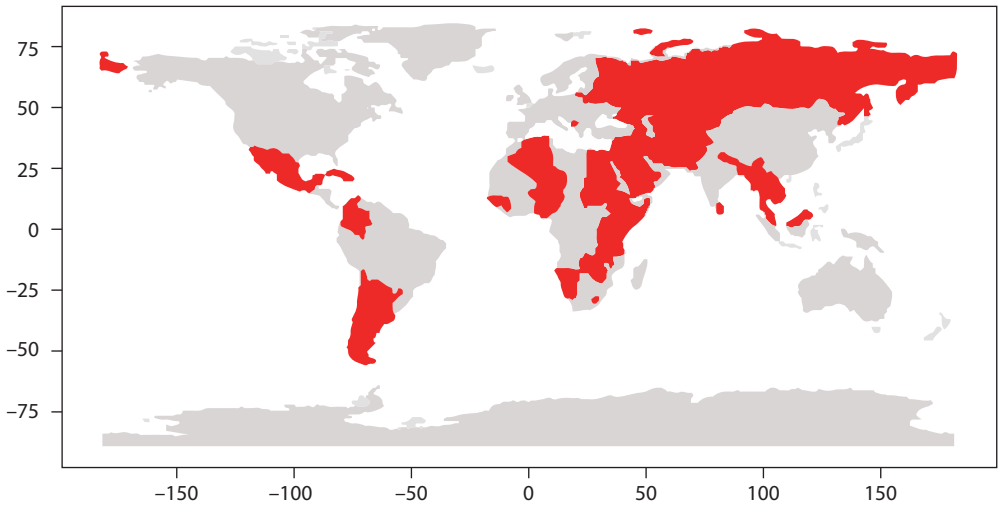


Figure 5: BRI Countries among Regular Governmental Participants of the WIC (Source: Own editing)

Unsurprisingly, members of the Shanghai Cooperation Organisation have been the most consistent participants throughout the whole decade, as they form a *de facto* alliance in promoting the norm of cyber sovereignty in international arenas like the UN General Assembly, and the leaders of those countries are often given the opportunity to make opening remarks at the World Internet Conference. In 2015, when Chinese President Xi Jinping attended the conference personally, he met with leaders of the Shanghai Cooperation Organization member states collectively. The Russian Prime Minister Medvedev remarked in his keynote speech that Russia had always advocated that all countries should have equal access to Internet management – as advocated by Xi – and that the work should be done

[32] Cyberspace Administration of China, 'Cyberspace Administration of China Launches the Initiative on China-Africa Jointly Building a Community with a Shared Future in Cyberspace' (Office of the Central Cyberspace Affairs Commission, 25 August 2021) <https://www.cac.gov.cn/2021-08/25/c_1631480920680924.htm> accessed 15 October 2024.

under the framework of the United Nations and based on the work of the International Telecommunication Union.[33]

China's persistent promotion of cyber sovereignty at the WIC over the last ten years, with discourses that align with those of the developing countries, especially those sceptical of the Western model, is influencing the rule-making associated with global cyber governance, leading to a more multilateral cyber governance landscape. The passing of UNGA Resolution 73/27 in 2018,[34] which established an 'Open Ended Working Group' to discuss the role of state government in global cyber governance, is a sign of this development. Among the 119 countries that voted in favour of the Resolution, 52 are frequent attendees of the World Internet Conference.

VI Conclusion

Despite a de facto boycott by Western countries and ongoing criticism and ignorance, China has been hosting the World Internet Conference consistently for a decade. From a general examination of its official documents and Chinese media reportage from 2014 to 2023 that used a natural language processing approach, the research finds that China has been leveraging the WIC to build strategic partnerships and alliances to promote a cyber sovereignty agenda and a state-primacy model of Internet governance to shape a favourable global cyber order by strategically using discourses acceptable to and alignment with the targeted audience.

The research finds that the Chinese government is developing the term 'cyber sovereignty' into a universal legal principle rather than a mere political slogan, and Chinese official discourses at the WIC emphasise the importance of non-interference and sovereignty, the positive role of state and governments, the positive economic implications of technological developments, and have a strong developmental and forward-looking orientation. China has been intentionally defining cyber sovereignty in a way that aligns with the Bandung Spirit of the Non-Aligned Movement, whose main points include respect for the principles of the UN Charter, respect for sovereignty, non-interference and non-aggression, to promote the mobilisation of support. Most of the governmental participants of the conference are from developing countries, especially those engaged in the Belt and Road Initiative and the Non-alignment Movement.

---

[33] Official Weibo of the News Center of the World Internet Conference, 'In Addition to Xi Jinping's Speech at the Opening Ceremony of the World Internet Conference, Let's Take a Look at What the Guests from Various Countries Said (Shijie Hulianwang Dahui Kaimushi Chule Xi Jinping Yanjiang, Kankan Geguojia Bin Doushuo Le Sha)' (The Paper) <https://m.thepaper.cn/newsDetail_forward_1409778> accessed 15 October 2024.

[34] Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly on 5 December 2018. A/RES/73/27.

China's advocacy of cyber sovereignty and a state-primacy Internet governance model through the World Internet Conference has by no means challenged a free and open Internet or contributed to the fragmentation of the Internet. The issue is particularly crucial for the developing world, which is at a critical point in determining its path to digitalisation and whose choices will significantly influence the future rule-making of global cyber governance. However, this research is limited to China's promotion strategies without examining the effectiveness of its influence and global reception, particularly those of the developing world. This gap should be addressed in future research.

Boris Kandov*

Regulatory Approaches for Algorithms on Online Platforms in the Digital Services Act

Abstract

With the seemingly rapid progression of technological development, algorithms are also becoming increasingly powerful and complex, not least due to the emergence of artificial intelligence (AI). While the AI Act is not yet applicable, a European Union law governing the use of algorithms on online platforms already exists that sets out the potential risks and challenges associated with their use. The Digital Services Act (DSA) introduces several new regulations concerning algorithm-based, automatic filtering systems into EU law that play a particularly important role for online platforms, as algorithms are used in these in the form of filter and recommender systems. These help with the moderation of content on platforms on the one hand and ensure a better user experience on the other. At the same time, their use is also associated with potentially negative implications and risks. For example, the spread of misinformation, hate speech and other harmful content on online platforms can have a significant negative impact on democracy and social cohesion. The Digital Services Act aims to ensure that algorithmic systems are used transparently and responsibly. In the analysis of the Digital Services Act, the paper primarily employs the method of word interpretation. This involved a detailed examination of the language used in the Digital Services Act, focusing on the specific terms and phrases within the legislative text. By scrutinising the context and usage of these keywords, the paper aims to uncover their precise meanings and implications.

Keywords: algorithms, algorithm regulation, DSA, Digital Services Act, recommender systems, moderation

* Mag. Boris Kandov, LL.M., Research Associate, Department of Innovation and Digitalisation in Law, University of Vienna. This paper was supported by the Jubilee Fund of the Austrian National Bank. ORCID iD: 0009-0006-9102-886X.

I Introduction

Online platforms, ie hosting services that store and publicly disseminate information on behalf of a user,[1] are increasingly in focus when it comes to content moderation and curation. It is now not unusual but rather standard practice to use technological measures such as algorithms to cope with the increasing pressure to identify and subsequently block, remove, monitor or filter illegal content in order to avoid potential liability.[2] Similar to the E-Commerce Directive,[3] the Digital Services Act (DSA)[4] also obliges platforms to remove illegal content expeditiously, as soon as they become aware of it in order not to lose their exemption from liability.

In addition to automated content moderation, the other area in which algorithm-based systems are used is that of recommender systems. These filter and classify the increasing flow of information and prioritise according to certain parameters that most closely match and appeal to users' interests. Such recommender systems can be found on e-commerce platforms such as Amazon, where products are sorted accordingly, or on dating platforms, for example. Entertainment platforms such as Spotify and Netflix and social media such as YouTube and Facebook use recommender systems to make personalised recommendations to their users based on their specific preferences. Due to their significance in terms of access to and the processing of information on online platforms, such algorithms have a major influence, which is accompanied by systemic risks that can manifest themselves, for example, in filter 'bubbles' of selected information.[5]

Obtaining access to information about algorithms has not been easy in the past because it has not always been available in a machine-readable format, especially in the case of recommender systems, which are usually not always documented in a meaningful way. In order to obtain more information, methods such as scraping or deploying the data-subject's right of access, which is available under the GDPR, have been used to date.[6]

---

1 DSA Article 3(i).

2 Niva Elkin-Koren, Maayan Perel, 'Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law' in Giancarlo Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020, Oxford) 669.

3 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1.

4 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

5 Natali Helberger and others, Regulation of news recommenders in the Digital Services Act: empowering David against the Very Large Online Goliath <https://policyreview.info/articles/news/regulation-news-recommenders-digital-services-act-empowering-david-against-very-large> accessed 15 October 2024.

6 Ben Wagner, 'Algorithmic Accountability: Towards Accountable Systems' in Giancarlo Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020, Oxford) 682.

Regarding copyright law, for example, this has been common practice for more than a decade with YouTube's Content ID,[7] but also with other music and video platforms that use automated systems to identify and manage content. More recently, such systems have also been used to address hate speech, disinformation, counterterrorism and other violence-related content. When photos are uploaded, for example, they are compared with the content of industry-wide databases such as Microsoft's PhotoDNA[8] to combat child pornography. In the fight against hate speech, numerous platforms now rely on a process in which texts are analysed based on their supposed toxicity and blocked when a certain threshold is reached.

One problem that exists, or has existed, is that traditional legal frameworks and processes have been ill-equipped to monitor the opaque and relatively effective nature of algorithmic content moderation. In particular, over-enforcement in the area of permitted expression *(overblocking)* on the one hand and lack of enforcement in relation to content that is actually unauthorised on the other pose problems that may ultimately pose a threat to the rule of law if traditional rule of law institutions do not provide sufficient tools.[9]

The algorithmic shift in terms of the governance and regulation of platforms is ultimately the result of technical developments as well as politics and public discourse.[10] The current rules of the DSA are the product of this public and political discussion and the EU's response to how providers of online platforms should deal with problematic content such as misinformation and hate speech. In addition to isolated national measures, such as the German Network Enforcement Act (NetzDG) and the Austrian Communication Platforms Act (KoPlG), which is no longer in force, the DSA has now been adopted as a comprehensive and directly effective EU-wide regulation.

The increasingly important questions of how to deal with issues such as hate speech or misinformation on online platforms, including cross-border hate speech, as well as algorithms that are often barely comprehensible (like a black box) but at the same time make a decisive contribution to the function of platforms, should be made more transparent – whether platforms should be allowed to regulate themselves was and remains a topic of public discourse that led to the DSA. The guiding principle is to reduce negative effects on democracy and social cohesion. Safeguarding fundamental rights such as freedom of expression and freedom of information is therefore essential while at the same time establishing a balance and a limit to hate online. Which mechanisms decide what can be expressed publicly and where the boundaries lie? One of the solutions will not simply be to trust supposedly smoothly operating algorithms and AI systems. It is not a given that topics

---

7 How Content ID works <https://support.google.com/youtube/answer/2797370> accessed 15 October 2024.

8 Microsoft PhotoDNA <https://www.microsoft.com/en-us/photodna> accessed 15 October 2024.

9 Elkin-Koren, Perel (n 2) 670.

10 Christian Katzenbach, Der „Algorithmic turn" in der Plattform-Governance. Die diskursive, politische und technische Positionierung von Algorithmen und KI als „technological fix" für komplexe Herausforderungen, (2022) 74 (19) Kölner Zeitschrift für Soziologie und Sozialpsychologie 285, DOI: https://doi.org/10.1007/s11577-022-00837-4

such as content moderation and governance will be addressed on online platforms at all. On the other hand, the law also expects platforms to take responsibility accordingly, as we have seen at least since the introduction of legislative acts such as the E-Commerce Directive and now the DSA.[11] Algorithms are a welcome technical solution as the responsibility of platforms increases, but their use is not unproblematic in various respects. The DSA is now proposing what a successful solution to these issues could look like in relation to algorithmic systems.[12]

It is important to realise the tension between automated processes and the need for transparency and accountability in algorithmic content moderation. Automated tools efficiently handle large quantities of data but operate opaquely, raising concerns about decision-making and legal implications. The current legislative trends prioritise technology deployment over human rights, risking transparency and accountability. However, new laws like the DSA aim to improve algorithmic governance by enforcing transparency, accountability and risk assessment. The challenge is to integrate these principles through collaboration among experts, lawmakers and technologists to ensure a balanced and ethical digital future.[13]

II Algorithmic Content Moderation, Recommender Systems and Profiling

In relation to online platforms, algorithms are particularly relevant in the context of content moderation. This algorithmic moderation can be summarised as governance mechanisms that structure participation in a community to facilitate collaboration and prevent abuse,[14] or more narrowly, as systems that classify user-generated content based on matches or predictions, leading to a governance decision and outcome (eg removal, geo-blocking or account deletion).[15]

Recommender systems are designed to make it easier for users to use a platform by suggesting content that they are likely to like. However, user-friendliness is only one side of the coin. Online platforms benefit, for example, through longer retention times and, therefore, more advertising potential or directly recommending to users what they should

---

[11] Gergely Gosztonyi, *Censorship from Plato to Social Media* (Springer 2023, Cham), DOI: https://doi.org/10.1007/978-3-031-46529-1_4

[12] Katzenbach (n 10) 285.

[13] Giancarlo Frosio, 'Algorithmic Enforcement Tools: Governing Opacity with Due Process' in Simona Francese, Roberto King (eds), *Crossing the valley of death: Driving forensic innovation in the 21st Century* (Springer 2024, Cham), http://dx.doi.org/10.2139/ssrn.4610556

[14] James Grimmelmann, 'The Virtues of Moderation' (2015) 17 Yale Journal of Law & Technology 42.

[15] Robert Gorwa and others, 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance' (2020) Big Data & Society (2020) 7, DOI: https://doi.org/10.1177/2053951719897945

buy. These recommender systems work best when they are also based on profiling. The DSA now also provides a legal definition of the term. A recommender system is defined in the DSA as 'a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed'.[16] It should be noted that this definition does not generally cover hosting services or intermediary services, nor online search engines, but only online platforms, and at the same time, is not limited to certain forms of information. The 'content-agnostic' approach also runs through the entire DSA and is already known from the E-Commerce Directive.[17]

Recommender systems and the algorithms behind them sometimes only work so well because they work with profiling. The DSA addresses the risk of profiling in several places and considers, for example, in its recital 68 in relation to advertising, that online advertising plays an important role in the provision of services by online platforms but can also entail considerable risks. Online platforms should, therefore, be obliged to ensure that users receive information about the main parameters used to decide which advertising is displayed to them. Users should be provided with conclusive explanations that explain the underlying logic and whether profiling is used.

Interest-optimised personalised advertising, which may target weaknesses, can have serious negative effects on users. Manipulative techniques have the potential to cause social harm to entire groups, for example, through disinformation or discrimination against certain groups. For this reason, providers of online platforms should be prohibited from displaying advertising based on profiling based on racial and ethnic origin, political opinion, religion, ideology, trade union membership, genetic or health data, as well as sex life or sexual orientation.[18]

The parameters of such recommender systems should be presented in a way that is clear and easy for the user to understand. These parameters should include at least the most important criteria used to determine which information is suggested to the user, as well as the reasons why the individual criteria are important. This also affects cases in which information is prioritised on the basis of profiling and the user's online behaviour.[19]

Very large online platforms (VLOPs),[20] in regard to their recommender systems, should consistently ensure that users of their service have alternative options concerning the most

16 DSA Article 3(s).

17 Sebastian Felix Schwemer, 'Recommender Systems in the EU: from Responsibility to Regulation?' (2021) 1 (2) Morals & Machines DOI: https://doi.org/10.5771/2747-5174-2021-2-60

18 DSA Recital 69.

19 DSA Recital 70.

20 DSA Article 33(1): 'online platforms and online search engines which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms'.

important parameters of their recommender systems that are not based on profiling.[21] This provision can be found in Article 38 DSA. The legal text requires at least one option for each of its recommender systems that is not based on profiling.[22]

Like the GDPR, the DSA can be considered an exemplary law since there have been attempts to regulate similar aspects of algorithms on online platforms around the world – for example, the US American Algorithmic Justice and Online Platform Transparency Act, which has been proposed but not yet enacted. Similar to the DSA, the introduced American law establishes requirements for certain commercial online platforms (eg social media sites) that withhold or promote content through algorithms and related computational processes that use personal information. Online platforms must disclose their collection and use of personal information and their content moderation practices; retain specified records that describe how the algorithms use personal information and assess whether the algorithms produce disparate outcomes based on race and other demographic factors in terms of access to housing, employment, financial services and related matters; employ algorithms safely and effectively; and allow users to access and transfer their personal information.[23]

III Obligation to Provide Information in Terms and Conditions

The first specific provision in relation to algorithmic decision-making can be found in Article 14(1) DSA. This stipulates transparency obligations with regard to the terms and conditions of providers of intermediary services in relation to information on content moderation and algorithmic decision-making.[24]

Providers of intermediary services, including online platforms, must provide information in their terms and conditions on any restrictions they impose on the information provided by users in connection with the use of their service. This includes information on all guidelines, procedures, measures and tools used to moderate content, including algorithmic decision-making. This must be written in clear, simple, understandable, user-friendly and unambiguous language and should be made publicly available in an easily accessible and machine-readable format; in other words, transparency obligations regarding content moderation, with explicit reference to algorithmic decision-making.[25]

The term 'algorithmic decision-making' should not suggest that there is a certain decision-making power to the algorithm itself, as algorithms have no autonomy. The

[21] DSA Recital 94.

[22] DSA Article 38.

[23] Algorithmic Justice and Online Platform Transparency Act, S. 1896, 117th Cong. (2021), <https://www.congress.gov/bill/117th-congress/senate-bill/1896> accessed 15 October 2024.

[24] Bissera Zankova, Gergely Gosztonyi, 'Quo vadis, European's Union New Digital Regulation Package?' (2021) (2) Business and Law 67–90.

[25] DSA Article 14(1).

legislator has merely adopted this common term. Algorithmic decision-making refers to any form of automated content moderation. Therefore, it does not have to be a particularly sophisticated algorithm that meets the criteria for consideration as 'artificial intelligence' as defined in the European Commission's AI Act (Article 3(1) AI Act in conjunction with Annex I). Any use of automated means is sufficient, even if these are based on a simple if-then programming logic.[26]

In the interests of transparency and user protection and in order to avoid unfair or arbitrary results, certain rules should be laid down with regard to terms and conditions. Providers of intermediary services should clearly state in their terms and conditions the reasons why they may restrict the provision of their services. These should then always be kept up to date. In particular, but not exclusively, this should include information on all guidelines, procedures, measures and tools used to moderate content, including algorithmic decision-making. Providers of intermediary services can also use graphical elements such as symbols or images in their terms of use to illustrate the main elements of the information obligations under the DSA. Providers should inform the users of their service in an appropriate manner in the event of significant changes to the terms and conditions, eg if they change the rules for the information permitted in their services or about other such changes that could have a direct impact on the users' ability to use the service, and thus also in the event of changes to the algorithms.[27] Even if some online platforms have already adopted this practice voluntarily in part and with varying degrees of intensity out of goodwill, it is to be welcomed that this has now been legislated and applies uniformly to all online platform operators in the EU.

If the service is primarily aimed at minors, which may be expressed by the design or marketing of the service or by the fact that the service is predominantly used by minors, special efforts should be made to make the terms and conditions easier for minors to understand.[28] This means that the algorithmic decision-making tools must also be clear for minors, which makes the already difficult task of explaining how complex algorithms work even more difficult.

VLOP providers are subject to stricter transparency requirements with regard to their terms and conditions. They should also provide their terms and conditions in the official languages of all EU Member States in which they offer their services. Furthermore, users should be provided with a compact and easy-to-read summary of the most important points of the terms and conditions.[29] The DSA leaves open whether this also includes information on the algorithmic recommender systems, but this can be assumed on the basis of a systematic interpretation.

---

[26] Benjamin Raue, 'Art 14 – Allgemeine Geschäftsbedingungen' in Franz Hofmann, Benjamin Raue (eds), *Digital Services Act* (Nomos 2023, Baden-Baden) 259.

[27] DSA Recital 45.

[28] DSA Recital 46 DSA and Article 14(3).

[29] DSA Recital 48.

IV Transparency of Recommender Systems

A central component of the business activities of online platforms is the way in which information is prioritised and presented on their online interface. This includes algorithmic recommendations, ranking and prioritisation of information, indicated by textual or other visual representations, as well as other types of curation of information provided by users. These recommender systems can have a significant impact on users' ability to access and interact with information online. For example, they can facilitate the search for content relevant to users and contribute to an improved user experience. They also play an important role in reinforcing certain messages, spreading information virally and encouraging online behaviour. According to the DSA, online platforms should, therefore, always ensure that users are adequately informed about how recommender systems affect the way information is displayed and how they can influence the way information is presented to users. The parameters of these recommender systems should be clear and easy to understand to ensure that users can understand how the information displayed to them is prioritised. At a minimum, these parameters should include the key criteria used to determine what information is suggested to the user and the reasons why each criterion is important, which explicitly includes profiling.[30]

The DSA does not specify what such important criteria might be. However, this is not unwise, as these can differ from platform to platform. For example, purchase history can be an important parameter on Amazon, while liking certain pages can be an important parameter on Facebook. In any case, it is also to be welcomed that platform operators now also must explain why the respective criteria are relevant so that users can better reflect on why they are presented with specific content. However, it remains to be seen, and the CJEU will have to decide sooner or later in what level of detail online platforms will have to explain this information. The overriding premise remains the requirement of transparency.

To be a little more specific, regarding transparency, the DSA also requires online platform providers that use recommender systems to clearly and unambiguously set out the most important parameters used in their recommender systems in their terms and conditions, as well as all options for users to change or influence these important parameters.[31] This must be done in clear language. The requirement for clear and understandable language is already known from the GDPR.[32]

The said important parameters include explanations as to why users are shown certain content or why certain information is suggested. The DSA also prescribes a minimum content for this, so these important parameters must at least include the criteria that are

[30] DSA Recital 70.
[31] DSA Article 27(1).
[32] Schwemer (n 17).

most important for determining the information that is suggested to the user on the one hand[33] and the reasons for the relative importance of these parameters on the other.[34]

If several options are available for recommender systems that determine the relative ranking of information provided by users, there must also be a function that allows users to select and change their preferred option, and this option must be directly available and easily accessible on the online interface.[35] The fact that this option, which is already offered by some platforms, is now legally mandatory is a positive development, particularly from the user's perspective.

Criticism can be expressed here, on the one hand, insofar as the DSA is sticking its neck out and creating the possibility of allowing mandatory third-party recommender systems on online platforms.[36] However, in this case, one should start thinking about whether this would already represent a fundamental dilution of the business model of many online platforms and interference with the fundamental rights of the operators of these platforms.

Furthermore, even if platforms provide useful information, it may be insufficient if hidden in terms of service. User research from the Centre for Democracy and Technology shows that users prefer information about recommender systems to be visual, interactive, personalised, and allow direct control over the system. This is not achievable through terms of service alone. It is preferable to include this information on a designated information page or transparency report.[37]

Also, the information provided by platforms may not be sufficient due to the ambiguous language of Article 27 DSA, such as unclear definitions of 'main parameters' or 'most significant criteria'. Platforms must be held to high standards to avoid 'transparency theatre'. For instance, simply saying that content is being shown because the end-user liked similar content does not offer meaningful insight into a recommender system's parameters. Additionally, platforms should disclose detailed information for expert audiences, including system design, key metrics and data usage, ensuring comprehensive transparency for different recipients.[38]

Furthermore, Article 27 DSA can be compared to Article 5 Platform-To-Business Regulation [Regulation (EU) 2019/1150, P2B Regulation]. It can be stated that the European legislator has provided the same level of algorithmic transparency for online intermediary services in Article 5 P2B Regulation and Article 27 DSA. However, this can be regarded as cumbersome. On the one hand, because the legislator uses different terminology in the

---

33 DSA Article 27(2)(a).

34 DSA Article 27(2)(b).

35 DSA Article 27(3).

36 Natali Helberger and others, *Regulation of news recommenders in the Digital Services Act: empowering David against the Very Large Online Goliath* (2021) <https://policyreview.info/articles/news/regulation-news-recommenders-digital-services-act-empowering-david-against-very-large> accessed 15 October 2024.

37 Maximilian Gahntz, Claire Pershan, 'Action Recommended: How the Digital Services Act Addresses Platform Recommender Systems' (27 February 2023) VerfBlog, DOI: https://doi.org/10.17176/20230227-185115-0

38 Gahntz, Pershan (n 37).

German versions of the laws (eg, *Hauptparameter* and *wichtigste Parameter*, but these do not occur in the English versions) and, on the other hand, because individual criteria are listed elsewhere: once in the general clause itself and once in the specification of the general clause.[39]

The central differences between the requirements of the P2B Regulation and the DSA, however, lie in the fact that the P2B Regulation defines the limits of transparency obligations [Article 5(6) P2B Regulation] and provides for a guideline competence of the European Commission [Article 5(7) P2B Regulation]. However, regarding the guidelines, this difference is not really relevant because they could also be made fruitful for the interpretation of Article 27 DSA due to their lack of legal norm quality. [40]

V Alternative Recommender Systems without Profiling for VLOPs

Providers of VLOPs that use recommender systems must offer at least one option for each of their recommender systems that is not based on profiling.[41] There is no mention in the DSA that recommender systems should not be based on profiling by default, as initially recommended by the European Data Protection Supervisor in respect to the DSA.[42] In any case, online platforms can use recommender systems with preset profiling. In the case of VLOPs, there is an alternative, according to the DSA, but users must still actively deactivate profiling if it is preset by default on the specific online platform. Recital 94 DSA indicates that the option to select the alternative without profiling should be accessible directly from the online interface on which the recommendations are presented. In my view, this means that in the relevant online interfaces of large online platforms such as YouTube and Facebook, for example, there should be an unambiguous and clear selection option in the feed, for example, in the form of a button or at least a drop-down menu, to select a feed that is not based on profiling but, for example, on a chronological timeline. In any case, this is technically possible. Since the income of many VLOPs is also largely due to profiling, the opt-out variant chosen in the DSA is certainly a less severe one.

VI Risk Assessment of VLOPs

The responsibilities of VLOP providers also include the careful identification, analysis and assessment of all systemic risks arising from the design, including algorithmic systems,

---

39 Sebastian Schwammberger, 'Zusammenspiel von Friktionen mit anderen Rechtsakten' in Björn Steinrötter (ed), *Europäische Plattformregulierung* (Nomos 2023, Baden-Baden) 261.

40 Schwammberger (n 39).

41 DSA Article 38.

42 EDPS, Opinion 1/2021 on the Proposal for a Digital Services Act <https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf> accessed 15 October 2024.

operation and use, of their services in the Union.[43] Such risk assessments should be carried out at least once a year and whenever new functions are to be introduced that are likely to have a critical impact on identified risks.[44] The minimum annual risk assessment is a good choice in times of rapid technological change, especially as each introduction of a major change entails a separate risk assessment anyway.

Among the systemic risks, Article 34(1) DSA includes, in an exhaustive list, the dissemination of illegal content,[45] any actual or foreseeable adverse effects on the exercise of fundamental rights, in particular, respect for human dignity, private and family life, protection of personal data, freedom of expression and information, including media freedom and pluralism, the prohibition of discrimination, the rights of the child and consumer protection,[46] any actual or foreseeable adverse effects on social debate, electoral processes and public security[47] as well as any actual or foreseeable adverse effects in relation to gender-based violence, the protection of public health, minors and serious adverse effects on a person's physical and mental well-being.[48] The EU legislator is clearly responding here to the events surrounding the 2016 US presidential election, among other things, and is making an important contribution to stability in the EU by naming systematic risks and the obligation to analyse these risks.

In such risk assessments of VLOP providers, particular attention is paid to the design of their recommender systems and other relevant algorithmic systems.[49] Although the vast majority of VLOPs[50] use algorithmic systems to moderate their content, select and display advertising and contacts, the factors 'systems for moderating content'[51] and 'systems for selecting and presenting advertising'[52] are listed separately, as much but not everything must necessarily be based on an algorithmic system when it comes to content moderation or the presentation of advertising. The risk assessment should also analyse whether and how risks are influenced by deliberate manipulation of the service offered. In particular, reference is also made to the possible methodology of non-authentic use or automated exploitation of the service.[53]

---

43 DSA Article 34(1).

44 DSA Article 34(1).

45 DSA Article 34(1)(a).

46 DSA Article 34(1)(b).

47 DSA Article 34(1)(c).

48 DSA Article 34(1)(d).

49 DSA Article 34(2)(a).

50 Parul Pandey, 'The Remarkable World of Recommender Systems' (2019) <https://towardsdatascience.com/the-remarkable-world-of-recommender-systems-bff4b9cbe6a7> accessed 15 October 2024; Ankit Jena, '4 Great Platforms That Use Recommendation System' (2022) <https://www.muvi.com/blogs/platforms-that-use-recommendation-system.html> accessed 15 October 2024.

51 DSA Article 34(2)(b).

52 DSA Article 34(2)(d).

53 DSA Article 34(2).

VII Risk Mitigation of Very Large Online Platforms

In addition to the risk assessment, providers of VLOPs are also obliged to take appropriate, proportionate and effective measures to mitigate systemic risks in accordance with Article 34 DSA, with a particular focus on fundamental rights.[54] In a demonstrative list, the DSA mentions here, among other things, adapting the design, features or functioning of their services, including their online interfaces,[55] adapting content moderation procedures, including the speed and quality of the processing of reports on certain types of illegal content, and, where necessary, rapidly removing reported content or disabling access to it, in particular in relation to illegal hate speech or cyber violence, and adapting all relevant decision-making processes and the means used for content moderation,[56] testing and adapting their algorithmic systems, including their recommender systems,[57] and adapting their advertising systems and adopting targeted measures to restrict or adapt the display of advertising in connection with the service they provide.[58]

The testing of the algorithmic systems is a risk assessment activity (Article 34 DSA) on the one hand; on the other hand, it is also part of risk mitigation activity according to Article 35(1)(d) DSA. However, until now, there have been no established control and test procedures and corresponding standards that are the subject of research and development in science and economy. The algorithmic systems can be adapted initially in relation to the test results. A large number of weaknesses in automated means are already known, for example, in filter technologies for identifying and possibly making illegal content inaccessible for the purposes of content moderation. Adaptation can also involve selecting a different algorithmic system, no longer having a certain function performed by such systems or strengthening the role of humans.[59]

In the context of content moderation, for example, a matching technique with perceptual hashing, ie a fingerprinting technology based on the comparison of reference files, can be dispensed with if considerable overenforcement, in particular the enforcement of non-existent rights, is identified. If the algorithmic system that is used is retained, its settings can be adjusted, eg the tolerance of the filter systems with regard to deviations. These determine, in particular, the risks of overblocking, ie making lawful content inaccessible due to alleged illegality ('false positives') or alleged violations of the platform's terms of use.[60]

---

54 DSA Article 35(1).

55 DSA Article 35(1)(1).

56 DSA Article 35(1)(c).

57 DSA Article 35(1)(d).

58 DSA Article 35(1)(e).

59 Katharina Kaesling, 'Art 34 – Risikominderung' in Franz Hofmann, Benjamin Raue (eds), *Digital Services Act* (Nomos 2023, Baden-Baden) 588.

60 Kaesling (n 59).

In general, this is also a welcome approach, as ultimately, the online platforms themselves will know best how to implement risk mitigation measures, so why not give them this task?

VIII Data Access and Control for VLOPs

VLOP providers shall make the data necessary for the monitoring and assessment of compliance with the DSA available to the Digital Services Coordinator or the Commission upon reasoned request.[61] For these purposes, VLOP providers shall, at the request of the Digital Services Coordinator or the Commission, explain the design, logic of operation and testing of their algorithmic systems, including their recommender systems.[62] It can be seen that the transparency requirement runs like a continuous thread through the DSA.

It is obvious that explainability and transparency can quickly reach their limits in connection with algorithms. We should therefore be careful and protect ourselves against the 'transparency fallacy'[63]. How this transparency will ultimately be guaranteed will probably only be decided by the CJEU.

IX Excursus: The Digital Services Coordinator

According to Article 49 para 1 DSA, Member States must designate one or more competent authorities responsible for the supervision of providers of intermediary services and the enforcement of the DSA. One of these authorities must then be designated as the Digital Services Coordinator. This coordinator shall be responsible for all matters relating to the supervision and enforcement of the DSA in the Member State unless the Member State concerned has delegated certain specific tasks or sectors to other competent authorities. The Digital Services Coordinator is, in any case, responsible for ensuring the coordination of these matters at the national level and for contributing to effective and consistent supervision and enforcement of the DSA across the EU.[64]

In Austria, this task is depicted by the already existing Austrian Communications Authority ('KommAustria'). Hence, no new Authority is created. The corresponding national implementation law, the Coordinator for Digital Services Act (KDD-G), came into force on 17 February 2024.

---

61 DSA Article 40(1).

62 DSA Article 40(3).

63 Miriam C. Buiten, 'Chancen und Grenzen „erklärbarer Algorithmen" im Rahmen von Haftungsprozessen' in Daniel Zimmer (ed), *Regulierung für Algorithmen und Künstliche Intelligenz* (Nomos 2021, Baden-Baden) 173, DOI: https://doi.org/10.5771/9783748927990-149

64 DSA Article 49(2).

X Power to Conduct Inspections of VLOPs

In the context of algorithms, it is worth mentioning that, during inspections, the Commission's delegated officials and other accompanying persons authorised by it shall have the power to request from the VLOP provider concerned access to information on and explanations of the organisation, functioning, IT system, algorithms, data management and business practices, and to record or document such explanations.[65]

Furthermore, during inspections, the officials and other accompanying persons authorised by the Commission, the auditors or experts designated by it, the Digital Services Coordinator, or the other competent authorities of the Member State on whose territory the inspection is carried out may request explanations from the VLOP provider concerned on the organisation, functioning, IT system, algorithms, data management and business practices and may interview its key personnel.[66]

Article 69(2)(d) DSA contains a power for the Commission to require the provider of a very large online platform to provide access to information on the organisation, functioning, IT system, algorithms, data management and business practices, as well as explanations thereof, and to record or document these explanations. This power can be explained above all by the specifics of digital companies, whose organisation, functioning and, in particular, technical infrastructure cannot be easily viewed, recorded and understood by outsiders.[67]

In this respect, the right of 'access' is likely to represent a special form of the general power of inspection pursuant to Article 69(2)(b) DSA – to a certain extent, it is the power of digital inspection. It is aimed at a comprehensive search of the addressee's digital assets, including outsourced cloud capacities and sensitive information such as the operational algorithms of the platform, which is carried out on site, although not limited to the information stored on site. However, the right to 'explanations' (and related records or documentation) goes beyond this and takes into account the fact that the architectures of complex digital platforms and search engines can prove to be 'black boxes' even for the Commission's experts and can make it difficult or even impossible to effectively enforce the related provisions of the DSA.[68]

Article 69(2)(d) DSA gives the Commission (only, but at least) a right to sufficient transparency with regard to the technical facilities of the platform or search engine relevant to the alleged infringements. The addressees of an inspection must, therefore, be willing and able to explain the relevant facilities to the Commission in a comprehensible manner, including the software architecture of the platform, which is probably typically at the centre of the inspection. The scope of this duty to explain is likely to require some clarification in

[65] DSA Article 69(2)(d).

[66] DSA Article 69(5).

[67] Christoph Krönke, 'Art 69 – Befugnis zur Durchführung von Nachprüfungen' in Franz Hofmann, Benjamin Raue (eds), *Digital Services Act* (Nomos 2023, Baden-Baden) 945.

[68] Krönke (n 67).

practice. However, in the interests of effective enforcement of the DSA provisions, it will be necessary to demand that providers cannot simply provide abstract explanations but must comply with the Commission's request with the desired degree of concretisation.[69]

XI Monitoring Actions in regard to VLOPs

In order to carry out the tasks assigned to it, the Commission may take the necessary measures to monitor the effective implementation of and compliance with the DSA by VLOP providers. The Commission may order them to grant access to their databases and algorithms and provide explanations.[70]

To ensure effective implementation and compliance with the DSA, the Commission is authorised, pursuant to Article 72 DSA, to monitor providers' adherence to their obligations. For this purpose, it may demand access to data and algorithms granted by the provider, as well as access to other essential information. To this end, it can also engage independent external experts and auditors who are appointed by the respective national supervisory authorities to assist with the procedure (Article 72(1) DSA). Further, all necessary documents should be provided, and any clarifications required should be furnished. The Commission may establish detailed rules regarding the modalities of the procedure (Article 83 DSA).[71]

XII Commission Support from the European Centre for Algorithmic Transparency (ECAT)

To support the Commission in enforcing the DSA, the Commission's Joint Research Centre has established a Centre for Algorithmic Transparency, which will support the Commission with technical and scientific expertise.[72] The ECAT supports the Commission's supervisory function with multidisciplinary internal and external expertise. The centre is based in Seville, Spain, and was officially opened in April 2023. An interdisciplinary team of data scientists, AI experts, social scientists and legal experts will work on evaluating algorithms and identifying and measuring systemic risks. The centre particularly supports the Commission in evaluations to determine whether the functioning of algorithmic systems complies with the obligations of the DSA for risk management by VLOPs and very large

[69] Krönke (n 67).

[70] DSA Article 72(1).

[71] Ranjana Andrea Achleitner, 'Durchsetzung: Befugnisse von und Zusammenarbeit mit Behörden' in Björn Steinrötter (ed), *Europäische Plattformregulierung* (Nomos 2023, Baden-Baden) 239.

[72] European Commission, 'Press Release, Digital Services Act: Commission is setting up new European Centre for Algorithmic Transparency' (2022) <https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-setting-new-european-centre-algorithmic-transparency> accessed 15 October 2024.

online search engines (VLOSEs). The aim is to centralise research activities concerning transparency and algorithms. The ECAT is part of the European Commission and is operated by the Joint Research Centre (JRC) – the Commission's internal science and knowledge service – in close cooperation with the Directorate-General for Communications Networks, Content and Technology (DG CONNECT).[73] As a research centre, ECAT will especially support the Commission in the evaluation of the functioning of algorithms used on VLOPs and compliance with the associated risk management obligations.[74]

XIII Conclusion

The DSA now forms the core law on algorithms on online platforms. The regulation does not specify the content of the code or the technical or content-related design of algorithms. Rather, the approach chosen is that of transparency obligations and verification options. This gives the respective online platforms a certain degree of freedom regarding the algorithms and recommender systems they use. At the same time, operators of online platforms must now also pay mandatory attention to the systemic risks addressed in the DSA. Many details are still open, such as the question of how specific processes will work in the event of reviews and to what extent transparency will actually be required on the part of online platforms.

In my opinion, the concept of the DSA is sound insofar as it is not aimed at regulating the type and structure of algorithms *per se* but rather focuses on the potential risks arising from their use. The wording is open enough to ensure that the law has a long shelf life. In the coming years and decades, we can certainly look forward to decisions by the highest courts on unclear formulations and regulations in the respective legal texts. The path taken by the DSA, with its transparency and accountability obligations in relation to algorithm-based systems, is, in any case, a suitable and well-considered path that does not inhibit innovation but rather provides it with an easy guideline by identifying systemic risks that need to be avoided.

[73] Achleitner (n 71) 236.

[74] European Commission (n 72).

Simona Veleva*

Digital Services Act: Anticipating Challenges in Regulatory Implementation

Abstract

The current article examines the legal aspects and challenges anticipated during the implementation of the Digital Services Act (DSA) into national regulatory frameworks. As the DSA represents a ground-breaking legislative initiative aimed at governing digital services within the European Union, this article explores some practical matters in terms of its implementation, the choices of the Member States countries concerning a Digital Services Coordinator (DSC), as well as potential hurdles faced by national regulatory authorities (NRA) in the implementation process, taking into account the right to freedom of expression, access to information, and the principle of liability exemption for intermediaries.

The research explores the legal implementation of the DSA across EU Member States, with a focus on the harmonisation of the act and the challenges posed by differing legal traditions and regulatory approaches, emphasising the importance of the European Commission in the regulation of very large online platforms (VLOPS) and very large online search engines (VLOSE), the current practices and the future tendencies in this regard. In addition, the article also examines some complex, specific tasks related to the enforcement of the DSA's provisions. The NRAs face specific technical and logistical challenges regarding their new monitoring competencies, which the article also addresses.

Keywords: Digital Services Act, regulation of intermediaries, freedom of expression, Digital Services Coordinator, Very large online platforms (VLOPs), Very large online search engines (VLOSEs)

* Dr Simona Veleva, Assistant Professor, American University in Bulgaria. ORCID iD: 0009-0001-5044-6380.

I Introduction

The rapid development of the digital market and information society services, especially intermediary services, has revolutionised how individuals communicate, access information, and conduct business. It has led to a whole new digital services package being prepared by the European Commission designed to address the challenges arising from these trends, making the European Union's (EU) market compatible with other global markets and, at the same time, harmonising the rules in all Member States. With the focus and primary intention of protecting the fundamental rights of users, the Digital Services Act (DSA)[1] is applicable to designated platforms with more than 45 million users in the European Union (this rule was established based on 10% of the EU population[2]), as of 25 August 2023. As of 17 February 2024,[3] the DSA has applied to all platforms and intermediary services. Therefore, all Member States need to make certain amendments to their own legislation in order to meet these new obligations and to further nominate and prepare compatible and adequate national regulatory authorities (NRA) which can apply the respective amendments.[4] The DSA has the ambitious goal of establishing clear rules and responsibilities for online platforms and service providers while promoting a safe, transparent and accountable digital environment. However, at the same time, DSA changes the regulatory landscape established by traditional legal paradigms. This task is not easy, given the vast area of regulation which DSA will enforce and in relation to several other legislative acts, some of which were recently adopted and which will also need to be properly applied, such as the Copyright Directive,[5] the Audiovisual Media Services Directive (AVMSD)[6] and the General Data Protection Regulation,[7] the upcoming European Media Freedom Act (EMFA)[8] and the

1 Regulation (EU) No 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

2 See DSA Recital 76 and Article 33.

3 See DSA Article 93(2).

4 See DSA Recital 110 and Article 3(n).

5 Directive (EU) No 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L130/92.

6 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), as amended by Directive (EU) 2018/1808 [2013] OJ L95/1.

7 Regulation (EU) No 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) [2016] OJ L119/1.

8 Commission, Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU COM (2022) 457 final.

recently adopted Artificial Intelligence Act (AI Act).[9] They all interact with this new act and impose new challenges concerning their proper application by national authorities. The current article examines these new challenges, addressing both legal and practical problems that national regulators will face. Applying the DSA will impose particular legal problems in terms of proper and timely enforcement. Such problems will be both procedural (for example, the need for judicial review regarding the final entry into force of administrative acts, which might require significant time) and substantive (for example, the need for changes in horizontal legislation to empower administrative bodies with new powers). Although traditional freedom of expression constructions are still intact, implementing DSA will require developing existing standards to cover different forms of expression in the online environment. The proper implementation of the DSA will only be effective if big platforms are cooperative and aim to properly comply with it and if Member States implement serious legal and administrative measures to address the challenges and ensure the national NRAs have enough tools to be competitive and provide effective, efficient and timely regulation. Further, the DSA and the problems related to it perfectly illustrate how freedom of expression has developed over the past decades due to technological development; therefore, traditional freedom of expression standards have also developed, changing how people communicate and participate in public discourse.

II Scope of Regulation of Internet Intermediaries

The primary legal framework establishing and guaranteeing freedom of expression on an international level within Europe is imposed through different international treaties, but mainly by Article 19 of the Universal Declaration of Human Rights (UNDR), Article 11 of the EU Charter of Fundamental Rights and Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which stipulate a clear path for Member States and a traditional relationship between the state and private individuals. In the practice of the judiciary, mainly the European Court of Human Rights (ECtHR), the regulation of freedom of expression is well described and developed and is centred around the 'three-part test' which state bodies (mainly NRAs and afterwards the court) apply to define illegal content: namely, whether a measure of public power (i) protects legitimate aims, (ii) is prescribed by law, and (iii) imposes only such restrictions and sanctions that are necessary in a democratic society.[10] This traditional construction, well defined by the case law of the different jurisdictions, is applicable to the online

[9] Commission, Proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts COM (2021) 206 final.

[10] Adrienne Stone, Frederick F. Schauer (eds), *The Oxford Handbook of Freedom of Speech* (Oxford University Press 2021, Oxford) 159–172.

sphere as well,[11] especially in recent years since NRAs have also expanded with greater responsibilities in relation to the online sphere. Back in 2018, the Council of the EU issued a recommendation on the roles and responsibilities of internet intermediaries.[12] On the EU level, the Audiovisual Media Services Directive expanded the scope of regulation of online content, especially when media service providers provide non-linear media services. Only a few years after its amendment in 2018, it became clear that both markets and users' behaviour had changed, and a new legal approach was necessary. This is also evident in the approach towards the stricter regulation of influencers, for example. As of 2024, eleven NRAs in Europe define influencers as non-linear media service providers[13] and regulate them using different approaches. Most of them consider it necessary to determine that services (channels) that exceed certain thresholds shall be considered mass media services. The Netherlands, for example, specifies a minimum of 100,000 followers or subscribers on one individual platform.[14] For Spain, the threshold is 1,000,000 followers, which number is determined by the population of the country itself (Spain's population is around 47 million people), and a new decree was adopted in May 2024 that defines so-called high-profile influencers.[15] It is clear that more Member States will follow suit in the coming years.[16] Therefore, the new EMFA will also play a crucial role, as it will be interrelated with all other pieces of legislation, and often in many Member States countries, executed by the same NRAs. All this is part of an extra layer of regulation, and in the doctrine, it is defined as secondary regulation that, unlike traditional primary regulation (regulation of content), stipulates content moderation rules. This changes not only the way the market is constructed but also how the entire social and political debate occurs. Slowly but steadily, it also changes the traditional construction of the exercise of power through which the state can interfere with individuals' private sphere to protect different legitimate values, also protected by law. This is because more and more responsibilities are imposed on private parties who will need to take active measures to restrict content based on the applicable legal acts. This is, however, a problem for the NRAs. They face more challenges because

---

11 See *Editorial Board of Pravoye Delo and Shtekel v Ukraine* no. 33014/05, ECHR, paras. 61–64, 5 May 2011.

12 Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies.

13 Analysis and recommendations concerning the regulation of vloggers. Subgroup 1 Consistent implementation and enforcement of the new AVMD framework (ERGA 2021), <https://erga-online.eu/wp-content/uploads/2021/12/ERGA-SG1-2021-Report-Vloggers.pdf> accessed 15 October 2024.

14 France further adopted a separate Influencer Act, Law No. 2023-451 of June 9, 2023, aiming to regulate commercial influence and combat abuses by influencers on social media.

15 Spanish Royal Decree 444/2024 of May 1, 2024, available at: <https://www.boe.es/boe/dias/2024/05/01/pdfs/BOE-A-2024-8716.pdf> accessed 15 October 2024.

16 European consumer laws such as the Unfair Commercial Practices Directive (UCPD) and Consumer Rights Directive (CRD) also apply to the commercial activities of influencers. These laws are designed to protect consumers from unfair or deceptive practices in commercial transactions, which can include influencer marketing activities.

the scope of regulation is inevitably expanding. While traditional monitoring is based on a decision or a signal and includes radio and television, along with the most popular non-linear media services, covering influencers will require a much broader scope and most probably also involve the use of AI in monitoring systems. However, AI tools are not equally developed in different EU languages, creating new problems related to the equal application of such tools and their effectiveness.

The third layer of regulation under EU law is defined as tertiary regulation, which includes the regulation of regulators.[17] The regulation of NRAs is essential for the prevention of misuse or misinterpretation of all these provisions, especially in terms of the general provision of the Directive on Electronic Commerce[18] (e-Commerce Directive) that prohibits Member States from imposing the responsibility for intermediaries to generally 'monitor the information which they transmit or store [and the] general obligation actively to seek facts or circumstances indicating illegal activity' (Article 15).[19]

These last two layers of regulation are developed and implemented in the Digital Services Act as well, which has the potential to truly reshape the media environment and especially the responsibility of the so-called Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) that are dominating large portions of the digital market but also have a huge impact on the way human rights are exercised, especially freedom of expression. The arrival of the DSA marks a new moment in addressing the challenges posed by the digital sphere.[20] Amending the e-Commerce Directive, without, however, revoking the liability regime for online intermediaries, is a product of efforts to ensure the safety, integrity and fairness of platforms and services, safeguard users' rights and foster a more transparent and responsible online community. The DSA is primarily focused on navigating new responsibilities for intermediaries and introducing new approaches to illegal content. At the same time, the DSA is trying to uphold the balance between innovation, freedom of expression and protecting individuals from online content and conduct. Its significance lies in upholding principles of human rights in the digital era and in its potential to revolutionise the digital landscape entirely. So far, no legal act has imposed a blanket rule

---

17 Joan Barata, *The Digital Services Act and its impact on the right to freedom of expression: special focus on risk mitigation obligations* (Plataforma en Defensa de la Libertad de Información 2021) <https://dsa-observatory.eu/2021/07/27/the-digital-services-act-and-its-impact-on-the-right-to-freedom-of-expression-special-focus-on-risk-mitigation-obligations> accessed 15 October 2024; Giovanni Sartor, Andrea Loreggia, *The impact of algorithms for online content filtering or moderation* (European Parliament's Committee on Citizens' Rights and Constitutional Affairs 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf> accessed 15 October 2024.

18 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1.

19 Gergely Gosztonyi, Andrej Skolkay, Ewa Galewska, 'Challenges of Monitoring Obligations in the European Union's Digital Services Act' (2024) (1) ELTE Law Journal 45–60, DOI: https://doi.org/10.54148/ELTELJ.2024.1.45

20 Ondřej Moravec and others, 'Digital Services Act Proposal (Social Media Regulation)' (2021) 14 (2–3) Studia Politica Slovaca 166–185, DOI: https://doi.org/10.31577/SPS.2021-3.5

for intermediaries to remove all illegal content, no matter what its nature. In parallel, DSA has implications for both online governance and societal well-being. This underscores the importance of having regulations during a period of technological advancement and digital transformation. However, its proper application by Member State authorities and the huge scope of regulation that needs to be covered also amplify differences in the chosen approach and raise some challenges which need to be addressed. Outlining these problems will enhance their understanding and ensure the proper application of the new legal provisions.

III Defining and Restricting Illegal Content

Probably the main and hardest goal of the DSA and the entire DSA package is actually creating a safer, more transparent digital environment in which malicious players do not have the tools and possibility to undermine democratic values and, in some cases, even the capacity to change and manipulate the public debate. At the same time, DSA seeks to limit harmful, illegal content by protecting various legitimate aims.[21] This would be possible if certain responsibilities were imposed not only on the intermediaries but also on the NRAs in the Member States, which would actually have to monitor and sanction them. However, defining and actually managing the restriction of illegal content is a difficult task, given the challenges of defining, interpreting and monitoring content and, at the same time, preserving the liability exception already mentioned [specifically noted in Article 3(4)(a) DSA]. The exception is also further defined and confirmed in Article 4 DSA, which prescribes that service providers are not liable for transmitted information when they did not initiate it, did not select the recipient, and did not select or modify the information contained in the transmission. At the same time, the main challenge will be to actually identify the illegal content.[22]

Some speech or content might not be illegal in some Member States but might be in others, and the proper navigation between these interpretations and the impact any removal might have is significant. This will be one of the hardest struggles, both for intermediaries but mainly for the regulators that have to monitor them. Implementing ambiguous provisions and applying them accordingly will be one of the main challenges for the NRAs, especially in terms of Article 17. DSA defines quite broadly the concept of 'illegal content'.[23] Recital 12 stipulates that illegal content is content that 'under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory

[21] Jens-Peter Schneider, Kester Siegrist and Simon Oles, 'Collaborative Governance of the EU Digital Single Market established by the Digital Services Act' University of Luxembourg Law Research Paper (2023) 9, 28–32.

[22] Gergely Gosztonyi, *Censorship from Plato to Social Media* (Springer 2023, Cham) 89, DOI: https://doi.org/10.1007/978-3-031-46529-1_6

[23] Rebecca Tushnet, 'Best Laid Plans: The Challenges of Implementing Article 17' (23 October 2023) JOTWELL <https://cyber.jotwell.com/best-laid-plans-the-challenges-of-implementing-article-17/> accessed 15 October 2024.

content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities'. The Recital further gives different and illustrative examples of illegal content (sharing images of child abuse or non-authorised use of copyright-protected material), but at the same time, proper interpretation of what can be defined as 'illegal hate speech' or 'unlawful discriminatory content' might differ widely from country to country, including given the local context, the specifics of the speech, and the cultural diversity.

Article 9(1) DSA prescribes an obligation for providers of intermediary services to remove or act against specific items of illegal content issued by national administrative authorities. Paragraph (2) stipulates some restrictions, noting that the order needs to be prescribed by law and associated with specific reasoning explaining why the content is illegal, but also, most importantly, that the 'territorial scope of the order … is limited to what is strictly necessary to achieve its objective'. Still, this strict limitation is also open to wide interpretation and raises the question of the type of criteria used. If the content is illegal according to the regulator or the court's jurisdiction, this does not mean it will be illegal in other Member States where the service or the information is accessible. At the same time, regarding graphic or video content, especially that which is copyrighted, this order should be applicable in all Member States. These issues need to be properly addressed, and they will be based on the specific content and the grounds for their unlawfulness. While a national regulator can decide on the legality of content only based on their own national law or interpretation of the EU law, other national regulators or jurisdictions might not consider it illegal. This factor was considered in a dedicated report by the European Parliament.[24] The parliament 'highlights that in order to protect freedom of speech […] hosting service providers should not be required to remove or disable access to information that is legal in the Member State that they are established in, or where their designated legal representative resides or is established'. This is the reason why, in most cases, geo-blocking will only occur in the country in which the respective authority issued the order, but the possibility for its wider application is still open. The European Commission explained that 'where a content is illegal only in a given Member State, as a general rule it should only be removed in the territory where it is illegal'.[25] However, disputes in interpretation might arise, including regarding hate speech and its proper definition, discrimination and disinformation. For all these reasons, it becomes imperative to adopt a unified approach towards non-linear media service providers within Member States. The AVMSD prescribes that an 'on-demand audiovisual media service' (ie, a non-linear audiovisual media service) means an audiovisual media service provided by a media service provider for the viewing of programmes at the moment chosen by the user and at their individual request on the basis of a catalogue of

[24] See Report on the Digital Services Act and fundamental rights issues posed, Committee on Civil Liberties, Justice and Home Affairs, A9-0172/2020 <https://www.europarl.europa.eu/doceo/document/A-9-2020-0172_EN.html> accessed 15 October 2024.

[25] See Commission, 'Questions and answers on the Digital Services Act' (2024) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348> accessed 15 October 2024.

programmes selected by the media service provider.[26] According to this definition, different NRAs include different types of services, but the main difference is that some include a wide range of online providers, including influencers, and others do not. At the same time, this definition is improved and enhanced by EMFA, which prescribes that 'media service' means a service as defined by Articles 56 and 57 TFEU, where the principal purpose of the service or a dissociable section thereof consists of providing programmes or press publications, under the editorial responsibility of a media service provider, to the general public, by any means, in order to inform, entertain, or educate.[27] This creates even more reason for all NRAs to expand and unify their scope of regulation. Only in this way can DSA be properly applied by a unified approach with regard to the legality of the content and actually achieve its aims. Otherwise, vast areas of speech in the online sphere will remain unregulated, giving space for 'forum shopping' in terms of regulation.

IV Platform Accountability

The European Commission adopted a series of designation decisions under the Digital Services Act, designating overall 24 VLOPs and VLOSEs as of July 2024.[28] Some of the latest decisions of the Commission involved platforms which clearly provide pornographic content (PornHub, Stripchat, XVideos, and XNXX) that were specifically added during the second wave of designated decisions. The forms of new compliance that these platforms need to adhere to would include, among others, much stronger protection of minors, user-friendly mechanisms to flag illegal content, analysis of the systematic risks and placement of mitigation measures, as well as the redesign of services in order to limit their content being viewed by children, providing more transparency and accountability. Compliance will need to involve serious measures for preventing minors from accessing content, given the accessibility that these sites enjoy right now. The supervision of these platforms will be a joint task of the European Commission and the Digital Services Coordinators of the Member States of Establishment. The Commission is responsible for the supervision, enforcement and monitoring of compliance of the VLOPs and VLOSEs in relation to the systematic risks and how big platforms will address them, but for everything else, the Commission

[26] AVMSD Article 1(1)(g).

[27] EMFA Article 2(1).

[28] Along with the designated VLOPs Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando, Shein, Temu and VLOSE: Bing and Google Search, on December 23, 2023, the new sets of designation decisions added PornHub, Stripchat, XVideos, as well as XNXX, which was added in July 2024. Full list of the decisions is available here: <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> accessed 15 October 2024.

and the national authorities share the competences.[29] For this reason, the Commission and the Digital Services Coordinators sign agreements concerning their coordinated efforts to regulate content. So far, agreements with France (Autorité de regulation de la communication audiovisuelle et numérique, Arcom), Ireland (Coimisiún na Meán), Italy (Autorità per le Garanzie nelle Comunicazioni, AGCOM), and the Netherlands (Autoriteit Consument & Markt, ACM) have been concluded. Both regulators and the Commission are intended to be supported by an outside body, the European Centre for Algorithmic Transparency (ECAT), which was launched in April 2023 by the Commission. Outsourcing monitoring and due diligence are also specific problems since the entire process of monitoring and sanctions is increasingly mediated, despite the fact that, in this case, the Centre is part of the architecture of the Commission. This creates the risk of limiting content without the possibility of challenging and restoring it fast enough – or the opposite: being unable to take down and limit disinformation or illegal content efficiently and promptly while it is spreading and creating harm. In this sense, DSA is a general tool for the entire accountability network, built up among all the actors involved in the governance of algorithms, shaped by application structures and the structures of control of algorithms.[30] Particular challenges will emerge in the future for platforms that have a significant number of users but do not reach 45 million or whose identification of the flow of users is hard to distinguish. Currently, there are a few appeals against the European Commission regarding the application of the DSA to them. Zalando filed a complaint,[31] and so did Amazon in two separate fillings. The first complaint[32] on 5 July 2023 raised allegations that Amazon's designation as a VLOP is based on discriminatory criteria and violates the principle of equal treatment. Amazon filed a claim on 6 July 2023, requesting interim measures by the President of the General Court to order the suspension of the operation of the contested decisions, arguing that the obligation to provide users with an option for every one of their recommender systems is not based on profiling, in accordance with Article 38 DSA, and, second, the obligation to compile and make publicly available the repository required by Article 39 of that regulation.[33] These types of problems should not be underestimated. Balancing platform transparency and the legitimate interests of platforms regarding the confidentiality of information will be an issue in the future that both the Commission and the NRAs must navigate in a way that does not undermine or set back platforms on the European market compared to those in other competitive markets.

---

29 Bissera Zankova, Gergely Gosztonyi, 'Quo vadis, European's Union New Digital Regulation Package?' (2021) (2) Business and Law 67–90.

30 Florian Sauerwein, 'Emerging structures of control for algorithms on the Internet. Distributed agency – distributed accountability' in Tobias Eberwein, Susanne Fengler, Matthias Karmasin (eds), *Media accountability in the era of post-truth politics* (Routledge 2019, London), 196–211, DOI: https://doi.org/10.4324/9781351115780-13

31 See Case T-348/23 (2023/C 314/13), *Zalando v Commission*.

32 See Case T-367/23 *Amazon v Commission*.

33 See Case C-639/23 P(R) Order of the Vice-President of the Court, 27 March 2024.

Additionally, in order to address all these new responsibilities that platforms have, they will be required to sign contracts with third parties, usually fact-checkers, not only in terms of combating disinformation but also in relation to general moderation. This is also one of the main obligations under the Code of Practice on Disinformation,[34] which the DSA strongly supports.[35] At the same time, this also raises serious concerncs regarding the core values of the right to freedom of expression. As a consequence, the platform Meta, for example, currently signs contracts with third parties that will provide fact-checking, and although in most countries, they are well-established organisations with a good reputation, the main problem of the manner of outsourcing arises. Outsourced monitoring operations may lack the contextual understanding or nuanced judgement necessary to accurately distinguish between permissible content and prohibited material. As a result, legitimate content could be erroneously targeted, leading to censorship or infringement of freedom of expression. Although fact-checkers will not be able to take down content, Meta will label it non-verified, and their algorithms will provide much less visibility.[36] Further, there is a risk of inadequate response to disinformation or illegal content. Delays in identification, assessment, and action may allow harmful content to be disseminated. Without prompt intervention, platforms may struggle to effectively contain the dissemination of false information or harmful materials. This can potentially undermine trust in the moderation process. Users and stakeholders may demand greater transparency and accountability from both platforms and external monitoring entities to ensure that decisions are made fairly, impartially and without bias.[37] The general problem of disinformation lies in its specific nature and the fact that, in essence, it is not illegal. At the same time, institutions, civic society organisations and other actors expect platforms and NRAs to be able to combat and limit it. This is a challenging task, and some scholars even talk about the structure of the Algorithmic Marketplace of Ideas,[38] which changes the traditional concepts of free speech and, in this regard, the need for and means of its lawful limitation, including through regulation.

In order to address these challenges, content moderation and users' rights should be given careful consideration in regard to the outsourcing process's implications. Platforms should establish effective mechanisms for oversight, review and appeal to safeguard against censorship and ensure due process. Moreover, cooperation between platforms, regulators and civil society organisations is essential when developing best practices and standards for outsourced monitoring that prioritise accuracy, fairness and accountability. Ultimately, a

---

[34] See Commission Communication on the European Democracy Action Plan COM (2020) 790 final.

[35] DSA Recital 106.

[36] About Fact-Checking on Facebook and Instagram <https://www.facebook.com/business/help/2593586717571940> accessed 15 October 2024.

[37] See Maayan Perel, Niva Elkin-Koren, 'Accountability in Algorithmic Copyright Enforcement' (2016) 19 Stanford Technology Law Review.

[38] Philip M. Napoli, *Social media and the public interest: media regulation in the disinformation age* (Columbia University Press 2019, New York) 138–146.

balanced approach is needed that upholds freedom of expression while effectively combating harmful content.

In this regard, it is interesting how Article 14 will be applied, which creates the obligation for the providers of intermediary services to provide much more transparent information in their terms and conditions, including information on any restrictions that they may impose. This also includes 'algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system'. Legitimate questions and concerns arise regarding its effective enforcement, especially algorithmic decision-making in relation to content review. As some scholars argue,[39] algorithmic decision-making appears to impose restrictions primarily relating to the scope of content aggregation. Platform liability is possible only through transparent, accountable and contestable decision-making undertaken through an algorithm that properly applies 'digital due process'.

In light of the DSA's emphasis on transparency and user autonomy, the terms of use should encompass not only algorithmic parameters for content aggregation but also for recommender systems. Article 14(1) explicitly refers to tools utilised in content moderation and, in this regard, excludes the sorting of information. Its primary objective is to prevent 'over-moderation' by platforms, thereby averting the unjustified removal of otherwise lawful content by providers during the filtering of material deemed illegal.

By enlisting online intermediaries as 'watchdogs', DSA effectively delegates online enforcement to algorithmic tools.[40] Still, it needs to be underlined that, unlike Article 17 of the e-Commerce Directive, hosting service providers are not obliged to use automated content moderation tools, and this was a vital part of the DSA adoption debate.[41] Further, the Regulation (Recital 58) outlines that if automated methods are used in the process of internal complaint handling systems, human review is necessary. This is an essential safeguard that is in place, but at the same time, such an approach raises the question of timely and prompt resolution.

Overall, coordinators must develop and refine moderation practices that effectively identify and remove such content without overstepping the boundary of censorship or infringing on free speech.

---

[39] János Tamás Papp, 'How the DSA Aims to Protect Freedom of Speech – With Special Regards to Section 14. of the DSA.' – Part I. (2024) Constitutional Discourse <https://constitutionaldiscourse.com/janos-tamas-papp-how-the-dsa-aims-to-protect-freedom-of-speech-with-special-regards-to-section-14-of-the-dsa-part-i/> accessed 15 October 2024; Lorna McGregor, Daragh Murray and Vivian Ng, 'International Human Rights Law as a Framework for Algorithmic Accountability' (2019) 68 (2) International and Comparative Law Quarterly 309, 331, DOI: https://doi.org/10.1017/S0020589319000046

[40] Giancarlo Frosio, Christophe Geiger, 'Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime' (2023) 29 (1–2) European Law Journal 31–77, DOI: https://doi.org/10.2139/ssrn.3747756

[41] European Parliament resolution of 20 October 2020 on the Digital Services Act and fundamental rights issues posed (2020/2022(INI)), point 13.

V Navigating Disinformation within the DSA Framework: Legal and Practical Considerations

One of the main goals of DSA is to address disinformation and to tackle and limit it. This is one of the hardest and most challenging tasks that the act prescribes. This challenge is evident from the Recitals, and namely, the act addresses online disinformation among illegal content and 'other societal risks' (Recital 2). Its limitation is part of the drive for a more predictable and trusted online environment (Recital 9). Recital 69 notices that 'in certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups'. However, DSA mainly establishes four categories of systematic risk, which should be assessed by the VLOPs and VLOSEs. The first is the dissemination of illegal content; the second is related to the actual or foreseeable impact of the service on the exercise of fundamental rights; and the third is the actual or foreseeable adverse effects on democratic processes, civic discourse and electoral processes, as well as public security. Finally, the fourth category is related to an 'actual or foreseeable negative effect on the protection of public health, minors and serious negative consequences to a person's physical and mental well-being, or on gender-based violence' (Recital 83). These risks may arise from coordinated disinformation, and platforms need to address them properly and promptly. Without a doubt, the war in Ukraine and Russian disinformation campaigns pose risks and threats to the European Union.[42] At the same time, DSA does not limit disinformation *per se*, and this is exactly the type of information that can be both legal and harmful. In this sense, disinformation might be considered illegal only in cases when it contravenes the nine legitimate aims prescribed by Article 10(2) ECHR or abuses rights[43] as prescribed in Article 17 ECHR in regard to the denial of the Holocaust[44] or crimes against humanity. Therefore, media regulators have so far applied Article 3 AVMSD and the general rule that obligates media service providers not to suffer the creation or provision for distribution of any programmes and any broadcasts inciting to national, political, ethnic, religious or racial intolerance, extolling or condoning brutality or violence, or any broadcasts which are adverse to, or pose a risk of impairing, the physical, mental, moral and/or social development of children. Though these obligations only apply to media service providers and not intermediaries in general, DSA prescribes in Article 34(2), the obligation for VLOSEs and VLOPs, when conducting their risk assessments, to take into account how the risks 'are

[42] Elena Sherstoboeva, 'Russian Bans on 'Fake News' about the war in Ukraine: Conditional truth and unconditional loyalty' (2024) 86 (1) International Communication Gazette 36–54, DOI: https://doi.org/10.1177/17480485231220141; Gergely Ferenc Lendvai, 'Media in War: An Overview of the European Restrictions on Russian Media' (2023) 8 (3) European Papers 1235–1245, DOI: https://doi.org/10.15166/2499-8249/715

[43] *Katamadze v Georgia* no. 69857/01, 02 February 2001; *Norwood v the United Kingdom*, no. 23131/03, 16 November 2004.

[44] *Garaudy v France* no. 65832/01, 24. June 2003; *Witzsch v Germany* no. 7485/03, 13 December 2005.

influenced by intentional manipulation of their service, including by inauthentic use or automated exploitation of the service, as well as the amplification and potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions.' Along with the Recitals, DSA implies that VLOPs and VLOSE must prescribe in their terms and conditions the specific prohibition of disinformation or disinformation campaigns (Recital 84). The absence of a standardised definition could lead to inconsistency in how platforms interpret and enforce moderation policies, resulting in a fragmented regulatory landscape. This could pose challenges for users and content creators seeking clarity on acceptable content standards, as well as for the responsible regulators, which in most cases are also the Digital Services Coordinators. To address these challenges, there is a need for clearer guidelines or definitions of disinformation within the DSA framework. This could help platforms develop more targeted and effective moderation strategies while safeguarding freedom of expression.[45] At the same time, it is imperative that NRAs only minimally intervene in the field of disinformation. Any measures should be the least invasive ones[46] and free of debate; empowering users and media literacy should be the main tools for combatting disinformation.

In summary, while there is a clear intention to address disinformation within the DSA, the lack of a standardised definition poses significant challenges for both platforms and regulators in terms of effectively moderating online content without inadvertently stifling free speech or promoting censorship.

VI Transparency and Accountability

In addition, transparency and accountability mechanisms play a key role in ensuring the effective implementation of DSA. Platforms should provide regular and comprehensive reports, which create further transparency and explain how systematic risks are approached and tackled. These reports should include a variety of factors, such as the number and types of items removed or flagged, the reasons behind removal actions and the effectiveness of prevention efforts. Transparent reporting not only builds trust in users and society but also makes it clearer and easier for users to address and protect their rights. This is one of the main achievements of DSA, and if applied properly, it can effectively change the way intermediaries function. It also balances the power between platforms and users. Still, the decisions of platforms need to be properly justified, and there should be a possibility for external review. In this regard, out-of-court settlements, as prescribed by Article 21 DSA,

45 Frosio, Geiger (n 40) 45.

46 Alain Strowel, Jean De Meyere, 'The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms?' (2023) 14 (1) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 1.

are a useful tool, and the DSC (Digital Service Coordinator) will have a serious task in certifying these special jurisdictions.

Protecting fundamental rights will be the main goal of these mechanisms,[47] including the obligation for VLOPs and VLOSEs to act reasonably quickly if notified by 'trusted flaggers' and to disseminate information to 'vetted researchers'. Although the criteria for both are established in the regulation, DSCs will require serious resources, and a grey area exists for interpretation when establishing both. Despite the detailed procedure prescribed in DSA, without full cooperation by the VLOPs and VLOSEs, neither mechanism will be very successful, and potential conflicts will be possible.

Notably, the DSA uses the term 'manifestly unlawful substances', which is defined as being 'evident to a layperson, without any substantive analysis, that the content is illegal or, respectively, that the notices or complaints are unfounded'. This definition is closely tied to the specific obligation of online platforms to suspend the processing of notices and complaints submitted through notice and action mechanisms and internal complaint handling systems [Article 23(2)]. Still, the term is quite vague, and different interpretations are possible.[48] Further, NRAs should be active players in these processes, identifying clear criteria for content removal and not delegating this role solely to intermediaries. This task will be challenging, and despite the new responsibilities of the EU Commission, it is up to the national regulators to take an active role in the communication and actual regulation of the content.

VII Need for Amendments in Horizontal Legislation and Proper Procedural Measures

The cornerstone in the proper and adequate application of the DSA lies in the appropriate amendment of numerous legal acts on a national level. Generally, most DSCs are also competent bodies under Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015, which lays down measures concerning open internet access and amends Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. This particular regulation is a vital part of the proper application of DSA since it requires end-users to have free access to information and content. Any restrictions will be applicable only if they are 'appropriate, proportionate and necessary within a democratic society, and if their implementation is subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms, including its provisions on

[47] Lani Watson, *The Right to Know: Epistemic Rights and Why we Need Them* (Routledge 2021, London).

[48] Mark D. Cole and others, *Algorithmic transparency and accountability of digital services* (European Audiovisual Observatory 2023, Strasbourg).

effective judicial protection and due process' (Recital 13). In this regard, since DSA is such a new instrument, deliberate procedures should naturally be adopted in other legal acts in terms of content regulation that are in compliance with the Audiovisual Media Services Directive, but also in the field of national security, criminal activities, etc.

Media regulation, especially after EMFA enforcement, will require precision and amendments to some of the national legal acts in order to avoid possible overlaps and to address the aims of the DSA.[49] The need for this is vital since right now, the penalties for online activities that are illegal (for example, in the field of non-linear media services or video-sharing platforms) are different (for example, fines) but rarely include removal of content. Hence, there should be special obligations for the respective administrative bodies responsible for the different sectors to require and ask the DSC to remove the illegal content on the respective legal grounds. Without proper adjustment in the other legal acts, which contain provisions safeguarding different legitimate aims, as prescribed in Article 10(2) ECHR, the adequate implementation of the DSA will not be complete. Such in-depth analysis is required in all Member States. Furthermore, in the process of content removal in accordance with Article 9 DSA, the path for a relevant national administrative authority to identify illegal content and then take appropriate measures to limit it is long and may be challenged before the court. Sometimes, court procedures can take significant time. Once the court makes a final decision, the DSC can very quickly issue the order and inform the intermediaries to take down a specific piece of illegal content. However, the entire procedure may take so long that the harm caused by the content is already realised in its full potential. Therefore, specific safeguards should be taken; for example, in a limited amount of cases, preliminary measures or expediting proceedings should be prescribed.

Although not all Member States have adjusted their legislation regarding the DSA, many have prepared internal amendments to meet the new criteria, distinguish the DSC, and implement the Regulation accordingly.

VIII Addressing Technological Challenges and Resource Allocation. Coordination with Other Competent Bodies

Finally, Digital Services Coordinators must address numerous challenges that are not strictly legal ones but are nevertheless essential to the proper application of the DSA. Recruiting and preparing qualified personnel with the requisite skills and expertise will be essential. DSA mentions the obligation for the Member States to guarantee enough resources for the Digital Services Coordinators and that they should 'have all necessary resources to carry out their

[49] Mark D. Cole, Christina Etteldorf, *Future Regulation of Cross-Border Audiovisual Content Dissemination. A Critical Analysis of the Current Regulatory Framework for Law Enforcement under the EU Audiovisual Media Services Directive and the Proposal for a European Media Freedom Act* (Nomos 2023, Baden-Baden) 92–106, DOI: https://doi.org/10.5771/9783748939856

tasks, including sufficient technical, financial and human resources to adequately supervise all providers of intermediary services falling within their competence'. In this regard, given that most Digital Services Coordinators are government bodies executing activities associated with electronic communications, their independence and financial sufficiency need to be further guaranteed by Member States. Only in a handful of countries did the legislator decide to appoint the media regulator as a DSC rather than the communication regulator, and this occurred mainly in the countries where the regulators converge. The possibility for a body under the executive power to limit content is possible only after close scrutiny, proper application of the international standards within freedom of expression and a judicial review. Even then, this is not recommendable since guaranteeing freedom of expression should remain the main task for Member States in their pursuit of a safer online environment. Nowadays, platforms have become the public arena for debate, especially political content, and they shift the entire philosophy underlying the public discourse. Still, NRAs have become part of this debate and should be involved only when the 'three-part-test' is applicable.

At the same time, continuous training and capacity building are essential to ensure that DSCs remain updated on the latest regulatory developments, technological advancements, and best practices in digital service management.[50] DSCs, however, especially in smaller Member States, can struggle to provide competative and adequate training and development. A multifaceted approach is necessary for addressing these challenges and building adequate capacity that responds to all these new responsibilities DSCs, as well as other responsible bodies, have to face. This requires staff training, building infrastructure and good collaboration with different stakeholders.

Further, the DSA is a unique piece of regulation in terms of the need for serious and extensive cooperation among different regulatory bodies that can identify any type of illegal content on a national level, cooperate with other regulators in other Member States, and simultaneously with the European Commission. This increases the difficult of its timely and effective execution and makes the role of the DSCs even harder.

Finally, for small and medium companies operating in different markets worldwide, it is becoming harder to navigate and comply with the numerous European acts that cover their services, especially in the digital realm. Although micro and small enterprises are excluded from applying the Regulation, they still have to meet numerous requirements, and administrative burdens should not hinder their growth. This is also an important consideration that the EU legislator needs to take into account, given the need for competitiveness in the EU market compared to other markets.

[50] Cole and others (n 48).

IX Conclusion

In conclusion, the DSA is a strong and imperative attempt at implementing an overarching approach to technological and market development in the digital sphere. The proper implementation of DSA will raise numerous challenges for the NRAs – especially for the Digital Service Coordinators who must coordinate the sanctions against illegal content. The difference in national legislations regarding the definition of illegal content, along with practical problems related to the timely and proper issue of a final order against illegal content, raise further problems for the DSC and further complicate the harmonised implementation of the DSA, potentially leading to delays and future struggles in enforcement and interpretation across Member States. Furthermore, effective coordination among Member States and the administrative bodies on a national level, along with the vast area of regulation that DSA covers, requires efficiency, serious resources, and a very good understanding of the purposes of the regulation with respect to human rights and especially freedom of expression.

In general, the complex legal framework is in fast-paced competition with the development of the market itself, and while more and more regulations and directives are adopted, the NRAs and the DSCs, in particular, need to adapt through adequate and intense efforts to respond to the attempts of the EU legislator to catch up with the sector. This complicates the digital environment, and the Parliamentary Assembly of the Council of Europe has even proposed a new Internet Ombudsman institution 'either as a separate body or by expanding the remit of an existing body such as a data protection agency, a media regulator, or a conventional ombudsman institution responsible for the protection of human rights'.[51] Such an idea might seem far away right now, but the online sphere and its regulation are indeed becoming challenging in many regards.

Addressing these challenges is only possible through collaboration between national NRAs, policymakers, the European Commission, civil society and business, but mainly with VLOPs and VLOSEs, which must comply with the regulation. This is the only possible approach that can lead to a balanced, effective and competitive market that respects and protects users and supports and further develops the intermediaries that shape the digital environment. The main conclusion, however, remains that NRAs have to adapt rapidly and effectively to the new realities. Content moderation has looked significantly different since the last amendment of the AVMSD in 2018 and will look much more different in 2028. Therefore, the Commission, Member States and NRAs must coordinate efficiently and simultaneously make deliberate efforts not to hinder the operation of the market from slowing down due to all these regulations and to protect human rights.

[51] Standing Committee of the Parliamentary Assembly of the Council of Europe, Resolution 2334 (2020), Provisional version, 'Towards an Internet Ombudsman institution', 15 September 2020, 6.

Tuba Eldem*

Decentralisation as Resistance: Web3's Potential in Countering Digital Censorship and Redefining Cyber Sovereignty

Abstract

The Internet, initially celebrated as a bastion of freedom and openness, is increasingly becoming a domain of control, surveillance, and regulation by both states and private entities. The rise of state control and regulation of the Internet, along with the private sector's expanding control over information, poses significant challenges to the ideals of freedom and openness that once defined the Internet. This article examines the transformation in Internet governance from a state of minimal regulation to a heavily controlled environment by both governments and corporations and explores how the blockchain technology and decentralised architecture underlying Web3 promise to redefine Internet governance and resist censorship. Through a mixed-method approach that synthesises insights from computer science, political science, and legal studies, the paper argues that public blockchains challenge Internet Corporation for Assigned Names and Numbers' (ICANN) traditional control over DNS and significantly reduce the ability of centralised entities to exert control over content and communication, thereby enhancing freedom of expression and resisting censorship. The ability of Web3 to fully realise this potential is, however, dependent on overcoming complex technical and regulatory challenges.

Keywords: Web3, blockchain, Internet governance, digital censorship, cyber sovereignty, decentralisation, information controls

* Dr Tuba Eldem, PhD, Director of the Center for Cyberspace Studies (FBUCyber), Associate Professor of Political Science, Fenerbahce University. ORCID iD: 0000-0001-6264-255X.

I The Digital Westphalia: The Rise of Sovereign Controls in Cyberspace

Initially, the Internet was considered an autonomous space free from state regulation and intervention. Yet over the last two decades, information controls, which refer to mechanisms to monitor, manage and regulate the flow of information online, have significantly expanded thanks to the centralisation of power in governments and big corporations. Governments increasingly regulate flows of information to maintain national security, preserve cultural norms and uphold or impose certain moral standards. The evolution of state control of information is analysed according to three distinct generations, each marking a significant expansion in the scope and depth of governmental control.[1] The first Generation of 'Blocking and Filtering' is characterised by direct censorship tactics, such as blocking access to websites, filtering content based on keywords, and disrupting Internet services at the ISP (Internet Service Provider) level. Techniques such as IP blocking, DNS tampering and URL filtering are relatively straightforward and involve the interruption of the flow of information at various points within a country's Internet infrastructure. They are aimed to prevent users from accessing specific pieces of content or entire websites deemed undesirable by a government or authority. While China's Great Firewall is perhaps the most well-known example, several other countries, such as Russia,[2] Iran,[3] Saudi Arabia, the Gulf,[4] Egypt[5] and Turkey,[6] have all implemented similar strategies to regulate and restrict the flow

---

1 Ronald J. Deibert, Masashi Crete-Nishihata, 'Global Governance and the Spread of Cyberspace Controls' (2012) 18 (3) Global Governance 339; Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press 2010) DOI: https://doi.org/10.1163/19426720-01803006; Jonathan Clark and others, *The Shifting Landscape of Global Internet Censorship* (Berkman Klein Center for Internet and Society Research Publication 2017).

2 Gergely Gosztonyi, 'Special Models of Internet and Content Regulation in China and Russia' (2021) (2) ELTE Law Journal, 87–99, DOI: https://doi.org/10.54148/ELTELJ.2021.2.87; Julien Nocetti, 'Contest and Conquest: Russia and Global Internet Governance' (2015) 91 (1) International Affairs 111–130. https://doi.org/10.1111/1468-2346.12189; Nate Maréchal, 'Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy' (2017) 5 (1) Media and Communication 29–41, DOI: https://doi.org/10.17645/mac.v5i1.808

3 Orkideh Safshekan, 'Iran and the Global Politics of Internet Governance' (2017) 2 (2) Journal of Cyber Policy 266–284, DOI: https://doi.org/10.1080/23738871.2017.1360375

4 James Shires, *The Politics of Cybersecurity in the Middle East* (Oxford University Press 2022, Oxford) DOI: https://doi.org/10.1093/oso/9780197619964.001.0001; Ram Sundara Raman et al, 'Measuring the Deployment of Network Censorship Filters at Global Scale' (2020) Network and Distributed System Security Symposium (NDSS) <https://www.ndss-symposium.org/ndss-paper/measuring-the-deployment-of-network-censorship-filters-at-global-scale> accessed 15 October 2024.

5 Bassant Hassib, James Shires, 'Manipulating uncertainty: cybersecurity politics in Egypt' (2021) 7 (1) Journal of Cybersecurity 1–16, DOI: https://doi.org/10.1093/cybsec/tyaa026

6 Tuba Eldem, 'The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security' (2019) 43 (5) International Journal of Public Administration 452–465, DOI: https://doi.org/10.1080/01900692.2019.1680689

of information online. The OpenNet Initiative conducted Internet filtering tests across over 70 nations, discovering signs of filtering in 45 countries.[7] This figure is probably growing rapidly as a growing number of countries are initiating content censorship related to child sexual exploitation, hate speech and terrorism-related content.

The second-generation controls saw deeper penetration by state agencies into the domestic sphere, enhancing their capacity to monitor and regulate the flow of information through a broad range of legal and regulatory measures. These methods often entail the participation or compliance of private sector entities, such as ISPs and social media platforms, and include the submission of content takedown requests, mandatory sharing of customer data and the enforcement of defamation and libel laws against online content.

The third generation of controls represents a qualitative leap in the strategies employed by states to manage, influence and control the information environment. This generation is characterised by an unprecedented expansion of state surveillance capabilities, both in-depth and reach, facilitated by technological advancements and the globalisation of data flows. Third-generation information controls have largely seen the expansion of the extraterritorial reach of state actors in cyberspace. Many states engaged in targeted surveillance, digital espionage and disinformation campaigns.[8] Russia has been involved in disinformation campaigns that have sought to influence elections and sow discord in other countries, notably in the events leading up to the 2016 US presidential election.[9] China has been reported to use advanced cyber capabilities not just for surveillance within their own borders but also for espionage and intellectual property theft from entities in the United States and other nations.[10] Many authoritarian states, such as the United Arab Emirates, Thailand and Saudi Arabia, have extended their extra-territorial intrusion largely thanks to the deployment of spyware technologies. An investigation by the New York Times revealed that NSO's dealings played a pivotal role in aiding former Israeli Prime Minister Benjamin Netanyahu to broker the Abraham Accords with Bahrain, Morocco and the UAE. Subsequently, these client states reportedly employed Pegasus not only to survey domestic opposition but also to engage in espionage against geopolitical adversaries.[11] The

---

7 https://opennet.net

8 Howard Nissenbaum, Bence Kollanyi, 'Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum' (2016) ArXiv, DOI: https://doi.org/10.48550/arXiv.1606.06356; Nigel Inkster, 'Information Warfare and the US Presidential Election' (2016) 58 (5) Survival 23–32, DOI: https://doi.org/10.1080/00396338.2016.1231527; Robert Chesney, Danielle Citron, 'Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics' (2019) Foreign Affairs 147–155.

9 Stephen McCombie, Adrian J. Uhlmann, Shane Morrison, 'The US 2016 Presidential Election & Russia's Troll Farms' (2020) 35 (1) Intelligence and National Security 95–114, DOI: https://doi.org/10.1080/02684527.2019.1673940

10 Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (eds), *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain* (Oxford University Press 2015, Oxford) DOI: https://doi.org/10.1093/acprof:oso/9780190201265.001.0001

11 Ronald J. Deibert, 'The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy' (2023) Foreign Affairs <https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert> accessed 15 October 2024.

use of spyware has extended to democratic states such as Greece, Hungary, Poland, Spain and Mexico. These disclosures have revealed state-sponsored cyber espionage targeting journalists and political adversaries – blatant proof of the penetration of surveillance practices across both autocracies and democracies.

II Surveillance Capitalism and the Rise of Corporate Controls in Cyberspace

On the corporate side, the growing demand for these offensive tools has led to the rise of a lucrative market for advanced spyware, surveillance tech and services. The spyware industry, now valued at approximately $12 billion annually, has emboldened not only the prominent Israel-based NSO Group but also other Israeli firms like Cytrox, Cyberbit and Candiru, as well as former players like Italy's Hacking Team and the Anglo-German Gamma Group.[12] This proliferation reflects the broader trends in surveillance capitalism in which wealth and power are concentrated in the hands of a few tech giants who commodify and exploit personal data obtained through surveillance for profit.[13] In today's data economy, companies like Google, Facebook, Amazon and Apple have grown into colossal entities partly because of their ability to leverage vast amounts of data. The concentration of data, resources and decision-making power within a small number of large tech companies is considered to be creating a new form of techno-feudalism, where individuals have limited control over their data (akin to land in feudal times) and are dependent on tech platforms for access to digital services and economic opportunities.[14] According to the techno-feudal model, tech giants such as Google, Facebook and Amazon, which collect vast amounts of data to target users with advertisements more effectively, are seen as the new lords with control over digital resources, data and infrastructure. The Cambridge Analytica scandal is a blatant indicator of how such power dynamics operate in practice. Social media platforms, such as Facebook, compile intricate digital profiles of users by covertly observing their online behaviours. These detailed profiles, which capture individual preferences, interests, and even vulnerabilities, are then commoditised and sold to political interest groups without the users' consent. These groups employ the data to craft targeted campaigns that subtly manipulate public opinion and voter behaviour.[15] The Cambridge Analytica scandal

[12] Ronald J. Deibert, Louis W. Pauly, 'Mutual Entanglement and Complex Sovereignty in Cyberspace' in Didier Bigo, Engin Isin, Evelyn Ruppert, *Data Politics. Worlds, Subjects, Rights* (Routledge 2019, London) 81–99.

[13] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).

[14] Yannis Varoufakis, *Technofeudalism: What Killed Capitalism* (Melville House 2024).

[15] Carole Cadwalladr, Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' (17 March 2018) The Guardian <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 15 October 2024.

underscored the potential for massive data misuse in the absence of stringent privacy controls.

Tech giants have also gained significant prerogatives in determining what content is seen, shared and suppressed. The private sector's role in controlling information has expanded alongside the growth of digital platforms. Companies like Facebook, Twitter and YouTube not only control vast amounts of data but also control the infrastructure and platforms through which information is disseminated and transactions are conducted. This makes them important gatekeepers of information, with the power to amplify or suppress content through algorithms. They have important prerogatives in the areas of content moderation, de-platforming and algorithmic prioritisation, which are often criticised for being opaque, inconsistent and biased.[16]

The mounting concerns over centralised control, data commodification and the erosion of privacy have catalysed interest in alternative structures for the Internet – paving the way for the emergence of Web3. Characterised by its decentralised architecture and blockchain technology, Web3 is posited by its advocates as the future of the web, promising censorship resistance, enhanced security, transparency and user control, thus countering the monopolistic and surveillance-driven practices of traditional tech entities. This shift is seen as crucial in restoring self-sovereignty and enhancing user privacy, providing a robust framework that counters the centralised models that currently dominate the digital landscape.

The following section will explore the foundational principles of Web3, emphasising the pivotal technologies and initiatives that underpin this transformative shift. It will largely rely on insights gained from the participant observation of tech and thought leaders working in the area of Web3 and open-ended interviews conducted at the DevConnect conference in Istanbul in November 2023, where the leading tech experts and blockchain innovators shared their perspectives on the challenges and possibilities inherent in decentralised web technologies. This discussion will highlight how Web3 could lead to a censorship-resistant Internet and more participatory Internet governance structure while also recognising the significant challenges that must be overcome to fully realise a shift towards greater self-sovereignty and enhanced privacy.

III Web3: Envisioning the Future of the Internet

Web3 is a marketing concept coined by Ethereum co-founder Gavin Wood in 2014 and has attracted significant attention from cryptocurrency enthusiasts, major technology firms and

[16] Gergely Gosztonyi, *Censorship from Plato to Social Media: The Complexity of Social Media's Content Regulation and Moderation Practices* (Springer 2023, Cham) 111–119, DOI: https://doi.org/10.1007/978-3-031-46529-1_8

venture capital investors since 2021.[17] Proponents of Web3 usually explain it by comparing it with its earlier versions. The first, referred to as Web1, covered the early 1990s to the early 2000s. It was a read-only Internet site, and users were passive consumers of content, such as web pages or encyclopaedia entries. This era was characterised by static HTML pages with minimal user interaction. Web2 emerged around 2004 with the rise of social media platforms like Google and Facebook, leading to a more interactive era with user-generated content. However, the Web2 era was riddled with centralisation as network effects and economies of scale led to a few companies building extreme wealth based on user data and targeted advertising.[18] This centralisation and the numerous scandals that followed created a backlash against the manner in which personal data was handled, setting the stage for the development of Web3.

The cypherpunks, a countercultural group of software engineers, cryptographers and philosophers who emerged in the 1990s, laid much of the philosophical groundwork for Web3. Advocating for strong cryptography and privacy-enhancing technologies, they played a pivotal role in fostering the ideals of self-governance, individual freedom and self-sovereignty that are central to Web3.[19] The technical infrastructure of Web3 began to crystallise with Satoshi Nakamoto's introduction of blockchain technology in 2008 through Bitcoin. This innovation fostered a trustless, transparent and secure method for transaction recording and verification on a decentralised network. The momentum for Web3 continued to build with the launch of Ethereum in 2015, which led to smart contracts – self-executing contracts with terms directly written into code.[20] That same year, the InterPlanetary File System (IPFS) was developed, further advancing the Web3 vision by supporting decentralised storage and file-sharing across various applications.

The initial adoption of Web3 technologies was largely driven by the cryptocurrency community recognising the potential for decentralised finance (DeFi) platforms that operate independently of traditional banking systems. However, the implications of Web3 extend beyond DeFi, influencing sectors like social media and content delivery. These decentralised applications provide alternatives to traditional models, offering benefits in terms of data integrity, user sovereignty and resistance to censorship. The following section discusses the underlying technologies of Web3 and how they are likely to challenge Internet governance and counteract censorship.

---

17 Amanda Cassatt, *Web3 Marketing: A Handbook for the Next Internet Revolution* (Wiley 2023, New Jersey).

18 Thomas Stackpole, 'What Is Web3?' 10 May 2022, Harvard Business Review, https://hbr.org/2022/05/what-is-web3> accessed 15 October 2024.

19 Kelsie Nabben, 'Web3 as 'Self-Infrastructuring': The Challenge is How' (2023) (January–June) Big Data & Society 1–6, DOI: https://doi.org/10.1177/20539517231159002.

20 Andrew McAfee and others (eds), *Web3: The Insights You Need from Harvard Business Review* (Harvard Business Review Press 2023, Boston).

IV How Web3 Fights against Censorship and Reshapes Internet Governance

Web3, often synonymous with the decentralised web, leverages blockchain technology to create an Internet where applications and platforms operate on a decentralised network of computers rather than relying on central servers.[21] This decentralised, immutable and peer-to-peer nature of Blockchain is fundamental to Web3's resistance to censorship. Blockchains on which Web3 architecture is built operate as a type of database that distributes its data across many computers, where every entry, known as a 'transaction', is transparent to all users. This transparency ensures that any attempt at censorship is visible to all participants, who can then challenge and debate such actions. Second, blockchains are shared and decentralised, meaning that multiple copies of the blockchain exist simultaneously on different computers. Third, blockchains are immutable, which means that once data is recorded, it cannot be altered or removed. This structure makes it difficult for governments or other entities to suppress information or revise historical records. Finally, blockchains operate on the principle of disintermediation, where decisions are made through consensus among participants without the need for an intermediary. Content moderation policies work according to these consensus protocols, such as Proof of Work (PoW) and Proof of Stake (PoS), requiring approval from the network participants. This collective agreement is key to preventing any single party from individually changing data for purposes such as censorship or manipulation. The inherent difficulty of modifying any data already approved by consensus without the majority of the network's endorsement makes blockchain highly resistant to tampering.

A second way that Web3 fights censorship is by decentralising the hosting and storage of online content. In Web2, most websites and applications rely on centralised servers that are owned and operated by a single entity. This makes them easy targets for censorship by authorities that can block access to these servers or pressure the owners to remove or modify content. In Web3, however, content can be hosted and stored on distributed networks of nodes that are run by various users across the globe. This makes it harder for anyone to censor or manipulate specific content since even if some nodes are taken down or censored, the data remains accessible elsewhere in the network.[22]

Web3 introduces promising structural and functional innovations that complicate the ability of censors to directly interfere with content access and distribution. In Web2, censors typically block access to content by targeting specific servers or content delivery networks (CDNs), intercepting DNS requests, or employing IP-blocking censors. The decentralised

[21] Stackpole (n 18) 18.

[22] Will Scott, *Censorship Resistant Web Applications* (PhD thesis, University of Washington 2018); Adem E. Gencer and others, 'Decentralization in Bitcoin and Ethereum Networks' in Sarah Meiklejohn, Kazue Sako (eds), *Proceedings of the International Conference on Financial Cryptography and Data Security* (Springer 2018) 439–457, DOI: https://doi.org/10.1007/978-3-662-58387-6_24

architecture of Web3, involving decentralised naming systems and distributed file storage systems, complicates many of these conventional interference tactics. Decentralised naming systems such as Ethereum Name Service (ENS), Unstoppable Domains (UD) and Handshake (HNS) offer resilience against traditional DNS blocking and domain seizures by distributing control across a network of users. They also challenge the contemporary model of Internet governance. The current Internet infrastructure is predominantly centralised around ICANN, which manages 13 logical DNS root name servers. This centralisation makes Internet communications vulnerable to sophisticated censorship tactics like DNS and IP blocking.[23] In contrast, decentralised naming systems use distributed ledger technology to extend control widely among network participants. This greatly diminishes the centralised points of control that could be targeted for censorship or to restrict information access.[24]

Web3 also embraces distributed file storage systems, such as the InterPlanetary File System (IPFS), which disperses content across a network of nodes. Unlike conventional web protocols that locate content based on its location (URLs), IPFS uses a content-based addressing system where each piece of content is uniquely identified by a hash. Thus, as long as the content is hosted somewhere on the network, it remains accessible to anyone who knows its hash. This structure not only makes the web more resilient against censorship and server failures but also ensures that content cannot be easily removed or blocked by any single authority or organisation.[25] This was vividly demonstrated in situations like the censorship attempts in Turkey and Catalonia, where distributed mirror technologies and IPFS were used to bypass government-imposed Internet restrictions. For example, IPFS played a crucial role in counteracting Turkey's censorship of Wikipedia by hosting the entirety of Turkish Wikipedia on its network. This initiative was part of the Distributed Wikipedia Mirror project led by the IPFS team, which aimed to make Wikipedia available in a decentralised manner.[26] Similarly, during the 2017 Catalan independence referendum, activists and organisers used decentralised and blockchain technologies to circumvent censorship and ensure the integrity and confidentiality of the voting process. They used IPFS to spread referendum-related content through a decentralised network, ensuring accessibility despite government blocks. Blockchain was also critical for recording votes in an immutable ledger, which strengthened the security and reliability of the election results.

---

[23] Joseph L. Hall and others, *A Survey of Worldwide Censorship Techniques* (1 November 2023) Internet Research Task Force <https://www.rfc-editor.org/rfc/rfc9505.pdf> accessed 15 October 2024.

[24] Juan Benet, *'Preventing Digital Totalitarianism. Modern Orwellian States'* (presented at the DevConnect, Istanbul, 18 November 2023).

[25] Ibid. Dennis Trautwein et al, 'Design and Evaluation of IPFS: A Storage Layer for the Decentralized Web' in *Proceedings of the ACM SIGCOMM 2022 Conference (SIGCOMM '22)* (Association for Computing Machinery 2022, New York) 739–752, DOI: https://doi.org/10.1145/3544216.3544232

[26] Arzu Geybullayeva, 'In Turkey, Mirror Websites Are Helping Users Reconnect to Wikipedia' (16 June 2017) The Wire <https://thewire.in/external-affairs/turkey-mirror-websites-helping-users-reconnect-wikipedia> accessed 15 October 2024; also see: Marcin Rataj, 'Distributed Wikipedia Mirror Update' (31 May 2021) IPFS Blog, <https://blog.ipfs.tech/2021-05-31-distributed-wikipedia-mirror-update> accessed 15 October 2024.

Decentralised applications enabled secure and transparent voting processes and made it challenging for the Spanish government to interfere.[27] This innovative use of technology not only safeguarded the referendum process but also demonstrated the potential of these tools in supporting democratic practices under restrictive conditions.

A third way Web3 challenges contemporary Internet governance and potentially reduces self-censorship is by providing users with greater anonymity and asserting their self-sovereignty and privacy through empowering user control over their digital identities and data. In the contemporary Web2 architecture, users often have to link their digital identities to personal information such as real names or phone numbers when creating accounts on social media platforms. This practice not only strips users of anonymity but also exposes them to extensive surveillance, tracking and profiling by platform operators and external entities. Furthermore, in this centralised system, the control over user data is largely in the hands of the platforms, which reserve the right to change, remove, or commodify user content according to their own terms and policies, often without obtaining explicit consent from the users.

In Web3, however, users can create pseudonymous or anonymous identities that are secured by cryptography and blockchain. They can also store their data and content on decentralised platforms that respect their privacy and self-sovereignty. Through blockchain-based naming systems, users can own and control their personal data associated with domain registrations without needing to reveal their identities publicly, which is often required in traditional DNS registrations. Users of decentralised naming systems have true ownership of their domains, unlike traditional DNS where the domain is essentially leased from a registrar. Once acquired, blockchain domains are controlled by the individual through private keys, meaning they cannot be revoked by a third party without access to those keys.[28] This empowerment extends to how data is used and shared, giving users full control over their online presence. This growing self-sovereignty over their data and anonymity could diminish self-censorship by reducing fears of being personally targeted for one's online activities.

In China, blockchain technology has already been used to counteract censorship. In 2018, an anonymous user implanted an open letter describing harassment by Peking University within an Ethereum transaction and subsequently shared it on the Ethereum

---

[27] Marta Poblet, 'Distributed, privacy-enhancing technologies in the 2017 Catalan referendum on independence: New tactics and models of participatory democracy' (2018) 23 (12) First Monday, DOI: https://doi.org/10.5210/fm.v23i12.9402; Manel Medina, 'Governmental Censorship of the Internet: Spanish vs. Catalans Case Study' (2020) 68 (4) Library Trends 561, DOI: https://doi.org/10.1353/lib.2020.0011; Vasilis Ververis and others, 'Understanding Internet Censorship in Europe: The Case of Spain' in N/A (eds), *Proceedings of the 13th ACM Web Science Conference* (Association for Computing Machinery 2021, New York). DOI: https://doi.org/10.1145/3447535.3462638

[28] Alex Preukschat, Drummond Reed, *Self-Sovereign Identity* (Manning Publications 2021, New York).

blockchain.[29] Despite censorship efforts on widely used centralised platforms like WeChat, the Chinese government could not remove the letter once it was uploaded to the Ethereum blockchain. This event not only underscores the resilience of public blockchains in protecting information but also signifies their ongoing role as a crucial tool for safeguarding free expression in the future.

Last but not least, proponents of Web3 argue that Web3 would address censorship through user empowerment and the enhancement of democratic governance and participation. On traditional Web2 platforms, decisions about content and user interaction are typically made by a small group of platform administrators or algorithms designed by a company, often leading to opaque and sometimes controversial moderation practices. Web3's governance model shifts control and decision-making from centralised authorities to the community of users. Web3 introduces a system where users directly influence the platforms and protocols they engage with. This is achieved through participatory governance mechanisms of blockchain-based decentralised autonomous organisations (DAOs), which enable transparent and trustless decision-making by allowing stakeholders to participate directly in governance processes within decentralised systems. DAOs are structures that utilise blockchains, digital assets and associated technology to allocate resources, coordinate activities and reach decisions. Defined as community-minded and code-driven hybrid organisations, DAOs are considered an alternative to traditional organisational forms through the publication of operational data to the general public and enabling members to participate in governance.[30] DAOs allow users to vote on initiatives, propose amendments, finance projects and receive incentives for their contributions to the digital ecosystem.[31] DAOs have experienced explosive growth – from a total value of treasuries at $380 million in January 2021 to an impressive $25.1 billion by December 2023, with participants increasing from 13,000 to 6.8 million.[32] This shift towards grassroots, community-led governance defies traditional hierarchical structures by encouraging inclusivity and collective decision-making. Thus, the transformative potential of Web3 lies not only in fostering censorship resistance but also in significantly reducing the barriers to democratic engagement and control over digital spaces, thereby democratising the Internet in true form.

---

[29] Keith Zhai, Lulu Yilun Chen, 'Chinese #metoo student use blockchain to fight censors' (24 April 2018) Bloomberg, <https://www.bloomberg.com/news/articles/2018-04-24/chinese-metoo-student-activists-use-blockchain-to-fight-censors?embedded-checkout=true> accessed 15 October 2024.

[30] World Economic Forum, *Decentralized Autonomous Organization Toolkit: Insight Report* (January 2023) <https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organization_Toolkit_2023.pdf> accessed 15 October 2024, 6.

[31] Jonathan Ruane, Andrew McAfee, 'What a DAO Can—and Can't—Do' in Andrew McAfeeand others (eds), *Web3: The Insights You Need from Harvard Business Review* (Harvard Business Review Press) 61.

[32] World Economic Forum (n 30) 6.

V Unpacking the Challenges of Web3 Technologies

While Web3 offers substantial benefits in combating censorship and enhancing democratic governance, its broader adoption is not without challenges that stem from both technical difficulties and legal and regulatory uncertainties. One of the most pressing challenges for Web3 technologies, particularly blockchain-based systems, is scalability. Most decentralised networks struggle to handle large volumes of transactions quickly and efficiently compared to centralised systems. For instance, Ethereum, the backbone of many Web3 applications, can only process about 15-30 transactions per second in its current state, whereas a centralised system like Visa can handle thousands of transactions per second. Solutions are being explored but are complex to implement and have not yet been fully realised at scale. Another challenge is related to technical complexity and user accessibility. Web3's infrastructure and applications can be complex for the average user and require a certain level of technical proficiency. This can potentially limit its accessibility and widespread adoption. A third technical challenge is to ensure interoperability between different layers of Web3 and across different platforms within the same layer.[33]

Web3 also need to address a set of regulatory and legal challenges as it operates in an essentially vague regulatory environment. Many states are still struggling with how to deal with blockchain, distributed ledger technology, cryptocurrencies, DAOs, DeFi, non-fungible tokens (NFTs) and other aspects of Web3. The lack of clear and consistent legal frameworks across different jurisdictions is the greatest challenge. There are also different interpretations concerning the applicable law with respect to transactions and assets recorded on the blockchain. The application of anti-money laundering and counter-terrorism financing regulations to crypto transactions is another challenge for the regulators as the decentralised and anonymous nature of many blockchain transactions poses significant enforcement challenges.[34]

Additionally, while Web3 advocates for greater user privacy and control over data, the public nature of blockchain technology can paradoxically lead to privacy issues. For example, transactions on public blockchains are traceable and permanently recorded, which can expose user activities and balances to anyone who cares to look. Advanced cryptographic methods such as zero-knowledge proofs are perceived as potential solutions but are still complex and not yet widely implemented. Furthermore, the irreversible nature of blockchain may conflict with 'the right to be forgotten' upheld in the General Data Protection Regulation

[33] Jared Ronis, 'Understanding Ethereum's Layer 1 and Layer 2: Differences, Adoption, and Drawbacks' (Wilson Center, 13 October 2023) <https://www.wilsoncenter.org/article/understanding-ethereums-layer-1-and-layer-2-differences-adoption-and-drawbacks> accessed 15 October 2024.

[34] Ioannis Lianos and others, Regulating Blockchain: Techno-Social and Legal Challenges (Oxford University Press 2019, Oxford); Andrea Bonomi, Matthias Lehmann, Shaheeza Lalani (eds), *Blockchain and Private International Law* (Brill 2023, Leiden), DOI: http://doi.org/10.1163/9789004514850

(GDPR).[35] Addressing these challenges requires not only technological innovation and development but also collaboration between stakeholders, including developers, users, regulators and academics, to ensure that Web3 technologies can deliver on their promise of open, free and secure Internet.

VI Conclusion

The rise of information controls by both states and corporations has significantly impacted the landscape of freedom of expression and privacy on the Internet. Over the years, the expansion of centralised power in governance and corporate entities has led to sophisticated mechanisms to monitor, manage and regulate the flow of information online. This has resulted in a paradoxical situation where the Internet, once a bastion of free expression, has become a controlled environment where user data is extensively surveilled and manipulated for profit and power. The evolution of such controls and the risk of growing digital authoritarianism have facilitated the search for alternative models that can restore and protect the fundamental rights of users. Web3, characterised by decentralised blockchain technologies, offers a compelling alternative to the traditional, centralised models that dominate digital spaces. These technologies unsettle traditional data management by distributing transactions and data across a network, thus complicating any attempts at censorship, as in the case of the Turkish ban on Wikipedia or manipulation, as in the Catalan referendum in Spain. The integration of Web3 into mainstream use will, however, require overcoming a set of technical challenges, including scalability, accessibility, interoperability and privacy. Additionally, it will necessitate a concerted effort among a diverse group of stakeholders – developers, users, policymakers and academics – to collaborate in creating a regulatory and operational framework that supports the adoption and growth of decentralised technologies.

[35] The right to be forgotten, enshrined in Article 17 of the GDPR, grants individuals the authority to request the deletion or removal of their personal data under certain conditions. This provision empowers individuals to control their digital footprint by allowing them to erase their data when it is no longer necessary, unlawfully processed, or when they withdraw consent. This right is not, however, absolute and must be balanced against other rights and obligations, such as freedom of expression and legal requirements. See: 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) [2016] OJ L119/1.

Roland Kelemen* – Joseph Squillace** – Richárd Németh*** – Justice Cappella****

The Impact of Digital Inequality on IT Identity in the Light of Inequalities in Internet Access

Abstract

This article investigates the relationship between the United Nations Sustainable Development Goals (SDG) and Internet access, focusing on how digital connectivity influences the achievement of these global objectives. This research examines digital inequalities in access, usage, skills and outcomes through a mixed-methods approach, including statistical analysis and case studies. The findings indicate a strong correlation between Internet access and progression towards the European sustainability goals related to education quality, gender equality and industry innovation. In particular, it can be shown that where Internet access indicators are lower, digital literacy and IT identity scores are also lower for society as a whole, impacting both the quality of education and social mobility, while simultaneously reducing the economic competitiveness of the respective state. We can also see that these societies have a more patriarchal approach, negatively impacting the social status of women (although the COVID-19 epidemic negatively impacted social resilience, too) while further harming progress towards the Sustainable Development Goal associated with education. Significant disparities are also identified, particularly affecting rural areas, women, children and marginalised communities. The article futher explores IT identity, revealing that a strong IT identity enhances digital inclusion and empowerment. Article results highlight the necessity of addressing digital inequalities to ensure the equitable

* Dr Roland Kelemen PhD, Associate Professor, Széchenyi István University, Deák Ferenc Faculty of Law and Political Sciences. ORCID iD: 0000-0002-5419-8425. Roland Kelemen: The article was supported by the University Researcher Scholarship Programme (EKÖP-24-4-II-SZE-72), funded by the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation Fund.

** Dr Joseph Squillace PhD, Assistant Professor, Penn State University. ORCID iD: 0000-0003-4227-5144.

*** Richárd Németh, Assistant Lecturer, Széchenyi István University, Faculty of Mechanical Engineering, Informatics and Electrical Engineering. ORCID iD: 0009-0004-2533-2375. The article was suported by the the University Researcher Scholarship Programme (EKÖP-24-3-I-SZE-54), funded by the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation Fund.

**** Justice Cappella, Graduate Research Assistant, Penn State University. ORCID iD: 0009-0009-9788-9582.

distribution of digital benefits and advocating for Internet access as a fundamental right essential to achieving global sustainability and Internet equality.

Keywords: technology inequality, digital inequality, IT identity, human rights to Internet access, misinformation, disinformation

I Introduction

As technology has become the bedrock of society and embedded itself into every facet of existence, it is more vital than ever to understand how technology as an artefact exists in society today. While each new integration of technology has enabled a level of individual success beyond our wildest dreams, there has been a parallel, more insidious realisation that needs immediate attention: a darker construct known as technology inequality. A lack of direct access to technology may also have unintended consequences, identified as online (in)equality. This phenomenon exists when individual end users experience technology differently, leading to differential levels of individual development and the creation of online identities (or IT identities) based on technology access, education and Internet exposure.

In examining technology inequality, Squillace and May[1] operationalise IT Identity Theory developed by Carter and Grover[2] to conceptualise the notion of IT identity as 'the extent to which a person views the use of a hardware device, software application or environment as integral to his or her sense of self'.[3] The adaptation of IT identity is built on structural symbolic interactionist identity theories and provides that an individual will reluctantly accept the online surroundings they find themselves in while internally adjusting truth in the absence of the physical equipment needed to verify data trustworthiness. This delineation illustrates the highly pervasive nature effects have on individuals without equal access to technology compared to those with it, while often struggling to locate essential physical resources necessary for sustaining life that exist a few 'clicks away' for individuals with a technological device connected to the Internet.

Technology inequality, which leads to the deficiency of an individual's IT identity, is a societal problem that must be addressed. The confluence of factors creating this phenomenon is the net result of a lack of Internet access as a human right for all end users. It is an instrumental component of the destructive nature and negative impact lack of Internet access has on individuals' quality of life. More importantly, it is critical to identify

---

1 May Bantan, Joseph Squillace, 'Privacy Inequality and IT Identities: The Impact of Different Privacy Laws Adoptions' (2022) AMCIS 2022 TREOs <https://aisel.aisnet.org/treos_amcis2022/21> accessed 15 October 2024.

2 Michelle Carter, Varun Grover, 'Me, My Self, And I(T): Conceptualizing Information Technology Identity and its Implications' (2015) 39 (4) MIS Quarterly 931–958, DOI: https://doi.org/10.25300/MISQ/2015/39.4.9

3 Michelle Carter and others, 'IT Identity: A Measure and Empirical Investigation of its Utility to IS Research' (2020) 21 (5) Journal of the Association for Information Systems 1315, DOI: https://doi.org/10.17705/1jais.00638

the severity of technology inequality in the regression of entire communities globally, as restricted Internet access may lead to barriers to education, technology and online awareness based on race and culture.

This article comprehensively examines the complex interaction between Internet access and the United Nations (UN) Sustainable Development Goals (SDGs). By examining key dimensions of digital inequalities and the role of IT identity, this research provides insights into how digital connectivity can promote sustainable development and reduce global inequalities. It also aims to explore the impact of the digital ecosystem on today's societies and its impact on quality of democracy through these concepts and related data.

II Methodology

A key objective of the article is to explore the link between the UN SDGs and Internet access. To do this, it is essential to take as complex a view of the digital ecosystem as possible, eg to look not only at Internet access but also at other quantitative indices that affect the functioning of this digital ecosystem and that can be linked to the individual. These metrics will then be used to demonstrate the qualitative relationship between a qualitative quadrant of quantitative indices and the corresponding social reality, along with the current state of SDG implementation. The purpose of this chapter is to describe the methodological steps used in this research, complemented by a subsequent chapter on the conceptual framework applied within.

The conceptual framework of this article is grounded in the premise that Internet access is a critical enabler of sustainable development. This perspective aligns with the arguments presented by the Internet Society[4] that emphasise the significance of the digital ecosystem in achieving the SDGs. Due to the dynamic change in the Internet landscape, the UN introduced a strategic initiative to increase online access and user sustainability in the 2000s, including the adoption of the non-binding Millennium Development Goals (MDGs). During this 15-year implementation period, the UN not only identified gaps where more attention was needed, they also acknowledged inefficiencies and inadequacies in the effectiveness of this implementation. The results of this strategy led to the creation of the UN's Sustainable Development Agenda (SDA) and Sustainable Development Goals, which were associated with a General Assembly resolution ultimately adopted by all UN member states (193) in 2015. The accepted general resolution sets out 17 SDGs connected to 169 task-specific objectives (targets) to be achieved through 232 identified and associated task indicators. The SDGs are defined in a holistic way, with the commitments they are attached

[4] Internet Society, 'The Internet and Sustainable Development an Internet Society contribution to the United Nations discussion on the Sustainable Development Goals and on the 10-year Review of the World Summit on the Information Society' (2015) 4 <https://www.internetsociety.org/wp-content/uploads/2015/06/ISOC-ICTs-SDGs-201506-Final.pdf > accessed 15 October 2024.

to intended to be implemented in a comprehensive, non-binding legal and policy-oriented way from the implementation date through the period until 2030.[5]

This article uses a multidimensional approach to explore the role of Internet access in achieving the SDGs, focusing on access inequality, usage inequality, skill inequality and outcome inequality. Access inequality pertains to the physical availability of digital technologies and Internet connectivity, reflecting disparities in infrastructure and affordability.[6] Usage inequality examines differences in how individuals use digital technologies, influenced by factors such as age, gender, education and socioeconomic status.[7] Skill inequality addresses the varying levels of digital literacy and competencies among individuals,[8] while outcome inequality considers the different benefits and opportunities derived from digital technologies.[9]

Data for this article were sourced from multiple reputable organisations, including the UN, the International Telecommunication Union (ITU), the World Bank and the European Commission. These sources provide comprehensive datasets on Internet usage, broadband subscriptions and various socioeconomic indicators. For instance, data on Internet usage rates and broadband subscriptions were obtained from the UN Economic Commissions and the ITU, which regularly publish detailed statistics on global digital access and usage patterns.

Using data sets from indices linked to each SDG and statistical data published by the above-mentioned organisations, the article examines the links between indicators of Internet access, digital literacy and IT identity and the achievement of each SDG. For example, the article analyses the proportion of Internet users in different countries and regions, tracking changes over time, and comparing these trends with progress on relevant SDG indicators such as quality of education (SDG 4), gender equality (SDG 5) and industry, innovation and infrastructure (SDG 9). These analyses will highlight the extent to which the quality of a given society's relationship with the digital ecosystem affects the feasibility of achieving the related SDGs for that state, as well as the impact the identified trends had on social resilience and quality of democracy.

Through the above analyses, the article provides insights into the contextual factors influencing digital inequalities and their impact on IT identity. This includes a review of

---

5 Gábor Kecskés, 'The Legal Meaning of Environmental Sustainability – Do the Ecological SDGs Have Legal Status?' (2023) 107 Chemical Engineering Transactions 482, DOI: http://doi.org/10.3303/CET23107081

6 Laura Robinson and others, 'Digital Inequalities and Why They Matter.' (2015) 18 (5) Information, Communication & Society 569–582, DOI: https://doi.org/10.1080/1369118X.2015.1012532

7 Eszter Hargittai, 'Digital Na(t)ives? Variation in Internet Skills and Uses among Members of the Net Generation' (2010) 80 (1) Sociological Inquiry 92–113, DOI: https://doi.org/10.1111/j.1475-682X.2009.00317.x

8 Alexander van Deursen, Jan van Dijk, 'The Digital Divide Shifts to Differences in Usage' (2014) 16 (3) New Media & Society 507–526, DOI: https://doi.org/10.1177/1461444813487959

9 Paul DiMaggio, Eszter Hargittai, 'From the Digital Divide to Digital Inequality: Studying Internet Use as Penetration Increases' 15/2001 Working Paper of Princeton Center for Arts and Cultural Policy Studies, DOI: https://doi.org/10.31235/osf.io/rhqmu

various literature, policy documents and case studies. For example, the research examines how digital inequalities manifest themselves in different socioeconomic contexts and how they affect individuals' ability to use digital technologies for education and economic development.[10] In doing so, it raises much-needed attention to the disproportionate negative impact digital inequalities have on vulnerable groups, including women, children and marginalised communities.

One critical aspect of the qualitative analysis was the concept of IT identity, which refers to how individuals perceive and engage with digital technologies. IT identity is shaped by personal experiences, attitudes and skills related to technology use.[11] The article explores how a strong IT identity can enhance digital inclusion and empowerment while a weak IT identity can exacerbate digital inequalities. This analysis was supported by case studies from various regions, highlighting the diverse experiences of individuals in navigating the digital landscape.

III Outline of Concepts Related to the Article

The purpose of this chapter is to provide an outline of the concepts and indices associated with the SDGs, which will be analysed in the remainder of the paper. Digital inequalities refer to the disparities in access to, use of, and benefits from digital technologies among different population groups. These inequalities manifest in various forms, including differences in Internet access, digital literacy and the ability to effectively use information and communication technologies (ICT). The concept of digital inequalities is closely linked to the broader notion of the digital divide, which highlights the gap between those with access to digital technologies and those without it.[12]

Access inequality pertains to the physical availability of digital technologies and Internet connectivity. This includes factors such as the availability of broadband infrastructure, the affordability of Internet services and the geographical location of individuals.[13] Rural and remote areas often face significant access barriers compared to urban centres, where infrastructure is typically more developed, and services are both more affordable and reliable.[14]

---

10 Ellen Johanna Helsper, A Corresponding Fields Model for the Links Between Social and Digital Exclusion' (2012) 22 (4) Communication Theory 403–426, DOI: https://doi.org/10.1111/j.1468-2885.2012.01416.x; Martin Hilbert, 'Digital Gender Divide or Technologically Empowered Women in Developing Countries? A Typical Case of Lies, Damned Lies, and Statistics' (2011) 34 (6) Women's Studies International Forum 479–489, DOI: https://doi.org/10.1016/j.wsif.2011.07.001

11 Royce Kimmons, George Veletsianos, 'The Fragmented Educator 2.0: Social Networking Sites, Acceptable Identity Fragments, and the Identity Constellation' (2014) 72 Computers & Education 292–301, DOI: https://doi.org/10.1016/j.compedu.2013.12.001

12 Jan van Dijk, *The Digital Divide* (Polity Press 2020, Cambridge).

13 Robinson and others (n 6).

14 Hilbert (n 10).

Usage inequality extends beyond mere access to include differences in how people use digital technologies. This encompasses the frequency of use, variety of applications and services utilised, and the purposes for which digital technologies are employed.[15] Usage inequality is influenced by factors such as age, gender, education and socioeconomic status. For example, younger and more educated individuals are generally more likely to use a broader range of digital services and applications.[16]

Skill inequality refers to disparities in digital literacy and competencies. Digital skills range from basic abilities, such as navigating the Internet and using email, to advanced skills like programming and cybersecurity.[17] Skill inequality can significantly limit individuals' ability to participate fully in the digital economy and society. Furthermore, those individuals lacking digital skills may find it challenging to access online services, secure employment in a digitally driven job market, or engage in digital learning opportunities.[18]

Outcome inequality reflects the differing benefits and opportunities that individuals derive from using digital technologies. These outcomes can include improved educational attainment, better job prospects, enhanced social connections and access to healthcare services.[19] Outcome inequality often mirrors and exacerbates existing social and economic inequalities, as those who are already disadvantaged in terms of education, income, or social status are less likely to reap the full benefits of digital technologies.[20]

IT identity, or digital identity, encompasses how individuals perceive and engage with digital technologies. It reflects the integration of digital tools and platforms into one's personal and social identity. IT identity is shaped by an individual's experiences, attitudes and skills related to digital technologies.[21] A strong IT identity can enhance a person's confidence in using digital tools, foster a sense of belonging in digital communities, and encourage ongoing learning and adaptation to new technologies. For instance, individuals who regularly engage with digital platforms and perceive themselves as competent users are more likely to integrate these technologies into various aspects of their lives, such as work, education and social interactions. Conversely, those with a weak IT identity may feel intimidated by digital technologies, limiting their use and reducing their ability to benefit from digital advancements.[22]

---

15 Hargittai (n 7).

16 Nicole Zillien, Eszter Hargittai, 'Digital Distinction: Status-Specific Types of Internet Usage' (2009) 90 (2) Social Science Quarterly 274–291, DOI: https://doi.org/10.1111/j.1540-6237.2009.00617.x

17 van Deursen, van Dijk (n 8).

18 OECD, 'Skills Matter: Further Results from the Survey of Adult Skills' (2016) DOI: https://doi.org/10.1787/9789264258051-en

19 DiMaggio, Hargittai (n 9).

20 Helsper (n 10).

21 Kimmons, Veletsianos (n 11).

22 Ove Edvard Hatlevik and others, 'Students' ICT self-efficacy and computer and information literacy: Determinants and relationships' (2018) 118 Computer & Education 107–119, DOI: https://doi.org/10.1016/j.compedu.2017.11.011

The relationship between digital inequalities and IT identity is complex and bidirectional. Digital inequalities can negatively impact IT identity by limiting exposure to and confidence in using digital technologies. Conversely, a strong IT identity can help individuals overcome some aspects of digital inequality by motivating them to seek out and utilise available resources and opportunities.[23] Addressing digital inequalities requires a comprehensive approach that considers access, usage, age, skills, outcomes and the development of strong IT identities among all population groups.[24] This holistic approach is essential for ensuring that the benefits of digital technologies are broadly and equitably distributed, thereby supporting the achievement of sustainable development goals and fostering global, inclusive digital societies.

IV The United Nations Sustainable Development Goals and Internet Access

In 2015, after the creation and adoption by the UN of the general resolution outlining the Sustainable Development Goals (SDGs), the Internet Society published in parallel a document pointing out that parts of the digital ecosystem (eg ICT products and broadband) are important elements in achieving the SDGs. For example, when discussing the emerging and evolving digital economy, it is important to understand that production, distribution and consumption depend on broadband connectivity while also realising that these economic segments provide the tools necessary for health and education, among other areas. For this very reason, organisations are extremely concerned that no specific SDGs are dedicated to the Internet or the ICT sector.[25] Such a narrow sustainability goal would not be expressive enough but creating a complex sustainability goal that covers the whole cyber or digital ecosystem should be considered and supported.[26]

In addition, each segment of the digital ecosystem is included in several SDGs, targets, or indicators associated with them. For example, in connection with quality education, Goal 4b states that participation in higher education should be increased for developing countries, with emphasis exclusively on African countries, specifically in the field of information technology. Target b of SDG 5 (gender equality) points to the need to increase the use of technologies that improve women's situation, particularly information technologies and to support women's empowerment in these areas. Goal 9 concerning industry, innovation and

[23] Neil Selwyn, 'Reconsidering Political and Popular Understandings of the Digital Divide' (2004) 6 (3) New Media & Society 341–362, DOI: https://doi.org/10.1177/1461444804042519

[24] Jan van Dijk, Kenneth L. Hacker, 'The Digital Divide as a Complex and Dynamic Phenomenon' (2003) 19 (4) The Information Society 315–326, DOI: https://doi.org/10.1080/01972240309487

[25] Internet Society (n 4) 4.

[26] Serena Clark and others, 'Including Digital Connection in the United Nations Sustainable Development Goals: A Systems Thinking Approach for Achieving the SDGs' (2022) 14 (3) Sustainability 1–13, DOI: https://doi.org/10.3390/su14031883

infrastructure – resilient, evolving and sustainable industrialisation – is now unthinkable and impractical without access to the innovative use and development of the digital ecosystem. Lastly, point 9(c) explicitly states that access to information technologies should be increased, with further efforts made to ensure universal, affordable access to the Internet in the least developed countries by 2020. Unfortunately, as we see from the indicators associated with the 17 targets, the latter is far from being achieved. Thus, although several organisations wish to define access to the Internet as a fundamental right (which position the authors of this paper share, especially in the sense that without it, the SDGs are unattainable), the guarantee of this at the global level is currently a dream and simply untenable on a global scale.

However, it can be clearly deduced from the data that state protocols intended to deliberately block access to the Internet violate fundamental human rights.[27] Targets 6 and 8 associated with SDG 17 can be interpreted as the culmination of the sustainability target for the digital ecosystem. Target 17.6 promotes collaboration and access to technologies, knowledge sharing and innovation in science, technology and innovation. Target 17.8 states that '…by 2017, make the technology bank and the science, technology and innovation capacity-building mechanism fully operational for LDCs and increase the use of basic technology, in particular, information and communication technology'.[28] Unfortunately, as can be seen, creating, revitalising and developing a global partnership for sustainability is unthinkable and essentially unfeasible without an improved digital ecosystem. These challenges indicate that a separate SDG for the cyber ecosystem would allow for more effective action in these specific areas, as confirmed and illustrated by the indicators presented below.

Some of the sub-indicators associated with SDG 17 provide a stark indication of how global access to the digital ecosystem has evolved since the adoption of the SDGs. For example, one indicator connected with Goal 17.8 looks at the evolution of the number of Internet users in each country. This indicator shows the proportion of individuals who have used the Internet from any location in the last three months. The data used to showcase this indicator are available from the UN Economic Commissions' data series. When analysing the European Union Member States according to this indicator, we see that since 2012, there has been a significant improvement. According to target indicator 17.8, the EU average is well above 80, and the Member States with the highest digital literacy rates scored close to 100 percent (eg Luxembourg, Denmark, Finland, etc.), with Italy having the lowest rate among EU Member States, at 71.8.[29] Furthermore, regarding Goal 17.8, the world's leading economic powers achieved the following scores: the United States 91.8, Canada 92.8, Japan

[27] 'Digital rights are vital for sustainable development' access now, 6 February 2020 <https://www.accessnow.org/digital-rights-are-vital-for-sustainable-development/> accessed 15 October 2024.

[28] Transforming our world: the 2030 Agenda for Sustainable Development <https://sdgs.un.org/2030agenda> accessed 15 October 2024.

[29] Internet users per 100 inhabitants <https://w3.unece.org/SDG/en/Indicator?id=76> accessed 15 October 2024.

91.1, Australia 85.1 and the United Kingdom 92.6.[30] In contrast, the global Internet user index is 67.9, while the index for African countries is 43.2.[31] Thus, relevant and tangible differences in access to the digital ecosystem can clearly impact the other SDGs (including those dedicated to this area and indicated above). These indicators also immediately channel into SDG 10, which has not been mentioned so far but is concerned with reducing access inequalities between countries.

In this respect, even acknowledging that we are at the start of this journey, it is still necessary to state the reality that there is a need to at least reduce the significant gap that exists between states and countries that refers to the clear and noticeably difference in digital ecosystems, both in terms of fundamental user access to the Internet and how users with access are permitted to use the associated online resources. This change is necessary for not only creating clarity but also resolving other related access objectives.

It may help to refine the significant differences stated above concerning Internet access and use by examining the indicator for target 17.6. This indicator measures the ratio of fixed broadband Internet subscriptions per 100 inhabitants. 'Fixed broadband Internet subscribers per 100 people is obtained by dividing the number of fixed broadband Internet subscribers by the population and then multiplying by 100.'[32] This indicator is very important because, in addition to the number of civil subscriptions, it also includes the number of broadband Internet subscriptions of economic operators, thus giving foreign investors an idea of the size of the digital ecosystem in the country. However, it may be misleading as this indicator does not measure the number of citizens with daily access to broadband Internet, but rather measures the number of subscriptions per 100 inhabitants. Even within the EU, the rates established by this indicator are no longer as high as those of the previous indicator. The EU average is between 30 and 40, with the lowest score for Poland, where just 22.7 per 100 inhabitants have broadband Internet access.[33] The figure is 37.4 in the United States, 41.2 in the United Kingdom, 42.1 in Canada, 35.2 in Australia and 35.96 in Japan. The global average of 18.43 has doubled within the past ten years, although the African average is still under 5.[34] In his 2020 report on the SDGs, the UN Secretary-General highlighted that fixed broadband Internet is almost non-existent in the least developed EU countries due to the

[30] The proportion of individuals using the Internet from the total population of the country <https://afri-res.uneca.org/apps/internet-usage-africa> accessed 15 October 2024.

[31] Internet penetration rate in Africa as of June 2022 compared to the global average. <https://www.statista.com/statistics/1176654/internet-penetration-rate-africa-compared-to-global-average/> accessed 15 October 2024.

[32] Metadata Glossary <https://databank.worldbank.org/metadataglossary/world-development-indicators/series/IT.NET.BBND.P2> accessed 15 October 2024.

[33] Fixed Internet broadband subscriptions per 100 inhabitants (any speed), per 100 inhabitants <https://w3.unece.org/SDG/en/Indicator?id=75> accessed 15 October 2024.

[34] Fixed broadband subscriptions (per 100 people) <https://data.worldbank.org/indicator/IT.NET.BBND.P2?view=map> accessed 15 October 2024.

high cost and lack of infrastructure.[35] Conversely, the case of China is interesting, where there is hardly any difference between the two measurements, with an Internet access rate of 52.2 and a broadband subscription rate of 41.35, meaning that in China, barely half of society has access to the online digital ecosystem, which obviously creates social fractures and class warfare among its citizens.

The broadband Internet access indicator figure is more telling than the previously identified SDG marker. When correlating broadband Internet access data, it is necessary to understand that a suitable device is required to connect to the Internet, and both are essential for work in the digital economy, education, innovation and research domains. This means that, in the long term, the almost complete absence of such broadband access in some countries will lead to an even greater gap with the countries of the economic centre.[36]

It can also be seen in the data that, in addition to the access in disparity among states, the lack of Internet access disproportionately affects certain classes of citizens. For example, limited or no broadband access significantly affects people from already vulnerable communities with low economic standing (according to financial income and wealth status), with extreme prejudice affecting women, children, ethnic minorities, users from rural populations and people with disabilities who are traditionally marginalised. In the field of basic education, one in four schools globally lacks essential services (water, electricity, basic sanitation), but the situation is even worse with regard to internet access (which is missing in one in every two schools), depriving the affected children of the opportunity for future social mobility. This realisation suggests the catastrophic deprivation of Internet access for adolescent students, severely reducing their future social mobility, minimising educational growth and limiting both technological and digital literacy.

It is also worth considering that while the average share of people in developed countries who use the Internet is above 80%, many do not have the digital skills required to adequately exploit the benefits of the online digital ecosystem nor respond to its threats. Further attribution occurs partly because even though a large share of people use the Internet, few users actually have adequate and permanent Internet access. This claim is borne out by the fact that only five countries that provide data report a greater than 75% share of citizens who are competent in at least three of the skills of communication/collaboration, problem-solving, security and content creation.[37]

As can be seen from the above, tackling digital inequalities is a challenge for all countries, even those nations with Internet access above the global average. Therefore,

---

[35] Progress towards the Sustainable Development Goals Report of the Secretary-General 28 April 2020, 19. <https://documents.un.org/doc/undoc/gen/n20/108/02/pdf/n2010802.pdf> accessed 15 October 2024.

[36] Immanuel Wallerstein, *World-System Analysis – An Introduction* (Duke University Press 2004, Durham and London).

[37] United Nations, '2023 The Sustainable Development Goals Report: Special edition. Towards a Rescue Plan for People and Planet' (2023) 20, 21, 47, <https://unstats.un.org/sdgs/report/2023/The-Sustainable-Development-Goals-Report-2023.pdf> accessed 15 October 2024.

the next chapter examines the impact the gap in access to the digital ecosystem has on these indicators in each global state society with above-average access. The authors' previous research[38] has shown that varied access to the digital ecosystem in the context of a transforming or transitioning economy and state can lead to both situational and long-term livelihood disparities, which ultimately threaten the accomplishment of SDG 16 and its sub-goal of peace and security.[39] Digital inequality creates social and security fault lines even within a developed state, highlighting the global need to reduce and ultimately eliminate these inequalities; failure to do so will eliminate all likelihood of success or attainment of the identified SDGs.

V The Impact of Digital Inequalities in the European Union on Society, Specifically IT Identity

If we look at digital inequalities in the context of societies in developed or more developed economic areas, the issue of IT identity becomes very important. In states and regions that are socially backwards (in terms of Internet access and broadband subscriptions), this is an extremely relevant factor, as individuals cannot successfully develop their social or individual IT identities. Meanwhile, within societies in advanced economic areas, digital inequality is clearly identifiable as a dividing factor. Jan van Dijk pointed out in work from 2020 that these 'breakpoints' can also be interpreted as an analytical aspect of the digital divide. They concern who has access to the digital ecosystem, what their characteristics are (income, gender, education, age, characteristics of where they live), how they access it (ie what they use it for and what skills they have in this area), and what types of technologies they have access to.[40] These criteria can be summarised as fiscal access (a quantitative characteristic) on the one hand and cognitive access (a qualitative characteristic) on the other.[41] The former, financial access, refers to access to technology, while the second, cognitive access, refers to intellectual capacity. Based on the concepts included in the previously referenced paragraphs, financial access identifies the availability of infrastructure (in this case, Internet access, its quality and the existence and quality of a connecting device), while cognitive access recognises the ability to interpret, use and exploit access in an appropriate way for social mobility. Thus, we can infer that a deficit in one of these

[38] Roland Kelemen, 'Cyberfare State modelljei: A digitális állam lehetséges irányai' in Ádám Farkas, Roland Kelemen (eds), *A fejlődés fogságában? Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai* (Gondolat Kiadó 2023, Budapest) 13–42.

[39] Ádám Farkas, 'The Status and Role of Law and Regulation in the 21st-Century Hybrid Security Environment' (2022) 11 (2) Acta Universitatis Sapientiae Legal Studies 113–124, DOI: https://doi.org/10.47745/AUSLEG.2022.11.2.07

[40] van Dijk (n 12) 1–3.

[41] Tibor Szarvák, 'A digitális szakadék mint új periféria-képző jelenség' (2004) 18 (3) Tér és Társadalom 59, DOI: https://doi.org/10.17649/TET.18.3.958

(ie, technological inequality) profoundly impacts the other (ie, IT identity). Moreover, this impact can be seen on social mobility and, from a societal perspective, on resilience and, not insignificantly, on the overall quality of democracy.

The relationship between these two indicators was exemplified by the Covid-19 pandemic, which accelerated the digital switchover in numerous areas, including the closure of educational institutions, the implementation of digital education and the introduction of the home office. Additionally, research has shown the existence of a tangible link between digital inequality in the EU and the resultant low level of IT identity in other countries or regions during the spread of the epidemic. For instance, in areas where Internet use was lower (conscious usage by end users), or unequal between social groups (male and female, age distribution, educational attainment), the virus was able to physically spread more rapidly and with greater severity than in states or regions where these inequalities were less relevant.[42] A report by Friedrich Ebert Stiftung that focused on inequalities in Hungary during the Covid-19 pandemic explicitly addressed the evolution of digital inequalities. The research found that 91% of individual users who were surveyed had household Internet access. It is worth noting that while the specific question that was asked did not focus on what type of Internet access this meant, other data related to the research was extensively collected for analysis. Of users with the highest Internet use who were surveyed, 60% were from lower-income households. Moreover, 83% of households reported having a computer, and 91% of users had a smartphone, with only 5.5% indicating they had no devices. This disproportion becomes greater in small villages located in the eastern or southern parts of the country. Significantly, only 16% of individuals living in difficult economic or poor financial circumstances had insufficient digital devices to facilitate the learning of children and the work of adults.[43]

It is also worth comparing how EU and national averages have evolved in this respect during the same period. In the EU, 90% of households reported having broadband Internet (fixed or mobile), encompassing 90% of respondents residing in large cities and 86% living in smaller rural areas. However, the variation is much higher for fixed Internet compared to mobile Internet. On average, in the EU, 76% of households have a subscription to either fixed or mobile Internet, while in the Netherlands, the rate is almost 100% Internet access for combined rural and urban users. In comparison, Bulgaria, Romania, Latvia, Lithuania and Italy each have a rate below 60%. It should also be noted that Finland has a very low rate, but this is compensated for by the high quality and coverage of mobile Internet, which does not significantly improve the average in other countries. The picture is further complicated by the fact that the proportion of people who connect to the Internet daily is smaller than

[42] Marta Borda, Natalia Grishchenko, Patrycja Kowalczyk-Rólczynska, 'Impact of Digital Inequality on the COVID-19 Pandemic: Evidence from European Union Countries' (2022) 14 (5) Sustainability 1–13, DOI: https://doi.org/10.3390/su14052850

[43] Éva Fodor and others, *Az egyenlőtlenségek alakulása a koronajárvány idején Magyarországon* (Friedrich Ebert Stiftung 2020, Budapest) 17–18.

this, at 80% on average in the EU, with some countries and smaller municipalities closer to 60%. These countries are roughly the same as those with low network coverage, most notably Romania and Bulgaria, where daily Internet access is below 80%, even in large cities. It should further be pointed out that, on average, for the EU as a whole, there is more than a 10% disparity between the daily Internet access of people living in rural areas (73%) compared to those living in urban areas (84%). Researching the figures in regard to technological inequality, the number of people with a laptop (desktop computers are not specifically mentioned in EU statistics) in the EU is nearly 60% in large cities, compared to 47% in rural areas. While true, in the previous noted countries where we have seen high rates, this is also the case for this category, with rates close to 80% in Denmark and the Netherlands (large cities) and above 70% in rural areas. In contrast, Romania (18% and 40%), Bulgaria (18% and 40%) and Italy (24% and 33%) are associated with the lowest figures.[44]

As we move from technology inequality indicators to IT identity (or cognitive) statistics, the EU has examined the proportion of citizens with skills above the basic level in information and data literacy, communication and digital content creation in three categories for each Member State. The aggregate data shows the EU average is 26% (one in four EU citizens have greater than basic skills in all three areas). In terms of metropolitan areas, Germany, Ireland, Spain, Croatia, Luxembourg, Austria, Sweden, Denmark, the Netherlands and Finland have rates above 40%. Bulgaria and Romania are far below the EU average in this category, where even in large cities, the proportion is below 15%. However, there is a relevant difference between rural and metropolitan areas in this category for all Member States. Looking at the individual categories, we obtain much higher rates, but Romania and Bulgaria are the two countries most behind in each category.[45]

It can also be observed that digital inequality and weak IT identity go hand in hand. EU statistics on digital inequalities confirm this, with the EU average of 58% of individuals banking online and the largest share in countries with the least digital inequality and the highest levels of IT identity. Meanwhile, the use of online banking services by Romanian and Bulgarian citizens is well below the average for the Member States. However, there is also very wide variation between urban and rural populations in this category as well, except for Finland, Denmark and the Netherlands, where the rates are almost identical. The largest difference in this category is Hungary, where 70% of the population in large cities use these services, compared to just over 42% in rural areas. Hungary has a similar relevant difference in IT identity (14% and 28%) between municipalities and the cities, so although the proportion of skills in the cities is above the EU average (but below the EU average in the metropolitan category), there is a marked overall gap in IT identity compared to the EU average. This categorical anomaly in Hungary is interesting because, on the technological

[44] EuroStat, 'Urban-rural Europe – digital society' (2022) <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Urban-rural_Europe_-digital_society#Individuals_.E2.80.93_frequency_of_internet_use> accessed 15 October 2024.

[45] EuroStat (n 44).

inequality side, there does not seem to be a huge difference compared to the EU average. Still, here we should refer back to the Friedrich Ebert Stiftung report, which points out that the eastern and southern regions of the country are lagging behind the central and western parts of the country, as confirmed by other research.[46]

In response to the negative impact and harm caused by digital inequality, the European Parliament adopted a resolution on 13 December 2022 aiming to reduce digital inequalities. The resolution states that 'whereas digitalisation can adversely affect people who lack sufficient digital skills or do not have access to an internet connection or to digital devices; whereas it may accentuate social differences by reducing some workers' opportunities to obtain quality employment.' However, this document points out that the EU has a relatively low digital competence rate; there is a digital divide in education in some Member States to the detriment of some students and teachers; 5.3% of school-age children are digitally deprived, and there are significant differences between the Member States. The action plans set out in the resolution essentially identify the need to achieve the sustainable development goals identified above: education, the inclusion of vulnerable social groups and the reduction of infrastructure gaps.[47]

VI Conclusion

It is essential that the goals for the digital ecosystem are formulated as a stand-alone sustainable development goal associated with a comprehensive policy framework. EU statistics point out that even in economically more developed regions, digital inequality and the resulting differences in levels of IT identity can generate significant social divides. The poorer regions (particularly Africa) are at a strategic disadvantage in this regard, making social mobility impossible for the rising generation. Providing users with increased global Internet access, ensuring online Internet access is a basic human right, and allowing all individuals to use the Internet, regardless of socioeconomic standing or status, is the first step to protecting end users. Pursuing this goal will aid in providing the requisite education necessary to prepare citizens to identify online threats, reduce their personal exposure online, and mitigate the spread and engagement of (mis)information and (dis)information at high levels.[48] This is necessary to save not only our fellow man but may be the only way to save democracy itself from the modern-day digital Fall of Rome.

---

[46] Anikó Fehérvári, 'Digitális egyenlőtlenségek Magyarországon' (2017) 26 (2) Educatio 157–168, DOI: https://doi.org/10.1556/2063.26.2017.2.1

[47] European Parliament resolution of 13 December 2022 on the digital divide: the social differences created by digitalisation (2022/2810(RSP)), [2023] OJ C177/57.

[48] János Tamás Papp, 'Recontextualizing the Role of Social Media in the Formation of Filter Bubbles' (2023) 11 (1) Hungarian Yearbook of International Law and European Law 136–150, DOI: https://doi.org/10.5553/HYIEL/266627012023011001012

Ádám Farkas* – László Vikman**

Information Operations as a Question of Law and Cyber Sovereignty

Abstract

The transmission of information content in the digital space, or its restriction, obstruction or distortion, is an extraordinary tool in the information age. States can be targets of information operations, regardless of their political system. For this reason, the ability and capacity to counter operations in the information space are fundamental issues for any state with a modern defence system. Information operations are, therefore, a necessary tool for the self-defence of sovereign states in the 21st century. However, the question arises as to what legal and institutional framework can provide an appropriate basis for information operations in such a way that the framework does not react to *ad hoc* events but ensures a systemic response in the long term while upholding the fundamental values of the state. The paper aims to contribute to understanding this problem by reviewing different nation-state solutions and providing a conceptual framework that synthesises legal, political, military and intelligence aspects.

Keywords: information operations, influence, cyber sovereignty, resilience, cognitive warfare

I Introduction

Technological developments in recent decades, such as the virtually limitless possibilities for communication, the continuity and speed of information flows and globalisation, have changed how individuals and society live their daily lives. Adapting to this has also been a major challenge for states in terms of interpersonal, economic and administrative relations. The security challenge is even greater. Both the legislature and the executive have a major

* Dr Ádám Farkas PhD, Senior Research Fellow, Széchenyi István University – Ludovika University of Public Service. ORCID iD: 0000-0003-2918-5267.

** Dr László Vikman, Assistant Researcher, Ludovika University of Public Service. ORCID iD: 0009-0002-1202-5769.

role to play in establishing and operating the appropriate regulatory framework. The fourth generation of warfare[1] is intrinsically linked to this accelerated and globalised system, as already evidenced by several international and non-international armed conflicts in the 21st century, as well as local conflicts, especially the Russo-Ukrainian war. However, beyond the dimension of statehood, the defence and security institutions of states must also reckon with the rise of non-state actors. One of the most striking novelties of hybrid scenarios is precisely the info-communication environment and its social, economic, political – and therefore security – embeddedness. However, this extends beyond the scope of warfare according to a much broader understanding of complex security and involves sub-threshold military operations and non-military operations.

Effective responses to contemporary defence and security challenges – mostly national security, military and law enforcement, but also affecting all segments of public administration – require an operational framework that is both adaptable to the specificities of the hybrid environment and provides the necessary guarantees. This is not a regulatory and operational challenge that can be solved by a targeted amendment to the law or by regulating specific issues that have been identified as priorities and otherwise maintaining the old ways of doing things. A change of mindset is needed. Another important specificity is that, given the nature of the challenges and threats, NATO allies, the EU and national regulation can only work effectively together. The concept of information operations (info ops) is, of course, not new in this context. However, its content and correlations, not least its scope, seem to be entering an era of deepening. It could be said that an 'information operations explosion' is taking place,[2] which is increasing the importance of the information space both for warfare and for influence and intervention outside it.

A legal-regulatory approach to this issue is of paramount importance for the rule of law, maintaining the values of the international community and operating within the rules and concerning the need for effective, systematic and consistent protection and action in the information space.[3] It is important, however, to put the issue under the spotlight of legal analysis in its own right, separately from fourth-generation warfare and hybrid threats,

---

1 For more details, see William S. Lind, Gregory A. Thiele, *4th Generation Warfare Handbook* (Castalia House 2015); William S. Lind, 'Understanding Fourth Generation War' (2004) (September-October) Military Review 12–16.

2 Mike Chapple, David Seidl, Cyberwarfare: *Information Operations in a Connected World.* (Jones & Bartlett Learning 2023, Burlington); Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Praeger 2017, Santa Barbara), DOI: https://doi.org/10.5040/9798400636431; Katharina Ludwig and others, 'Divided by the Algorithm? The (Limited) Effects of Content- and Sentiment-Based News Recommendation on Affective, Ideological, and Perceived Polarization' (2023) 41 (6) Social Science Computer Review 2188–2210, DOI: https://doi.org/10.1177/08944393221149290

3 Talita Dias, 'Limits on Information Operations Under International Law' in T. Jancárková and others (eds), *15th International Conference on Cyber Conflict: Meeting Reality* (CCDCOE 2023, Tallin) 345–363; Tsvetelina van Benthem, Talita Dias, Duncan B. Hollis, 'Information Operations under International Law' (2023) 55 Vanderbilt Law Review.

and to make it the subject of more intensive investigation beyond pre-existing studies.[4] It should be seen that this phenomenon of change also has implications for state and legal theory, whether in relation to the idea of cyber sovereignty[5] or the cyberfare state. The validation of the latter phenomena could significantly impact the design of more concrete state responses and the developments needed to shape them, as could the new meaning of information superiority.[6]

These kinds of theoretical questions significantly broaden the horizon of response. Without a broader spectrum of interpretation and, with it, planning, organisation and action, not only may the effectiveness of active operations be called into question, but the lack of adequate situational awareness and the reduced effectiveness of defence mechanisms may result in a serious disadvantage in terms of responding to counter-actions. A purely technical approach and the adaptation of old cognitive schemas and various rules to a new technical environment may easily lead to maladaptive solutions. In view of this, it is necessary to consider the possible legal responses to information operations within a complex framework. This framework must take into account sovereignty issues, defence-security specificities, the functioning of information operations and the structure of law as a system. All of this must be integrated into the very complex matrix of resilience in the context of social justice since the main impact of information operations is on society, whether the operation is military, intelligence or other.

Our main hypothesis is that legal responses to information operations should be adapted to complex security environment and that the different solutions should be linked to each other and then to the issue of resilience. To support this, we draw on literature, policy, strategic and regulatory sources, with the aim of identifying general lines of action for adequate protection against information operations. This may form the basis for further research on the topic.

Our analysis proceeds using three main sections. First, we review some of the main contexts of information operations. We use three subsections to increase understanding of the military-security perspective, and we outline the definitions of NATO on the matter and the always-evolving conceptualisation of these activities, the most state-of-the-art

---

4 See, for example: Oxford Institute ELAC, 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities' <https://www.elac.ox.ac.uk/the-oxford-statement-on-the-regulation-of-information-operations-and-activities> accessed 15 October 2024; Eian Katz, 'Information Operations in International Humanitarian and Criminal Law: Reflections on the Oxford Statement' <http://opiniojuris.org/2021/07/22/information-operations-in-international-humanitarian-and-criminal-law-reflections-on-the-oxford-statement/> accessed 15 October 2024; Waseem Ahmad Qureshi, 'Information Warfare, International Law, and the Changing Battlefield' (2020) 43 (4) Fordham International Law Journal 901–937.

5 Sean S. Costigan, 'Sovereign or Global Internet? Russia and China Press for Cybercrime Treaty' (2021) 20 (2) Connections QJ 9–13, DOI: https://doi.org/10.11610/Connections.20.2.01

6 Ádám Farkas, 'The Status and Role of Law and Regulation in the 21st-Century Hybrid Security Environment' (2022) 11 (2) Acta Universitatis Sapientiae, Legal Studies 113–124.

of which is cognitive warfare. In the following subsection, we briefly review the elusive approach to sovereignty in cyberspace, which will be difficult to capture (with significant consequences) due to the current rather diverse state practices and which, precisely because of these diverging interests, is not expected in the near future. We conclude the first chapter by presenting a proposal for a specific set of criteria to be followed in the context of the state regulation of information operations. In the second main section, we argue that, in addition to legislative and administrative instruments and hard state responses, individual and group-level resilience, which is increasingly important in security matters, must also play a role in countering the activities of counter-acting actors in the cognitive space. In the concluding reflections in the summarising third main section, we argue first and foremost that, in addition to identifying possible regulatory directions and pursuing a comprehensive analysis, efforts are needed to embed this in a comprehensive view of resilience.

With our article, we aim to stimulate professional dialogue and debate that, through a multidisciplinary approach but grounded on the basis of positive law, can develop definitions, frameworks, control and governance mechanisms that will allow states to guarantee a high level of national security proportionate to the threat while respecting fundamental human rights.

II Contexts for Information Operations

The importance of the information operations environment is due to the prominent role that info-communication has attained among the civilian population. Thus, the importance of cooperation with civilians regarding military and non-military threats has been enhanced. This, in turn, has increased the weight of the cognitive orientation on the military side concerning the technological approach to information operations. The phenomenon of 'sub-threshold' crises resulting from hybrid threats (in which, in addition to the military element's embeddedness in the population, cooperation with administrative, law enforcement and national security actors and the strengthening of state and civilian resilience play a prominent role), also has a bearing in this direction. In this context, it is also worth taking into account that the legal aspects of active and passive (operational) activities in the information space, including counter-actions, share the fate of other legal issues related to hybrid threats and new forms of warfare.[7] The character of 'sub-threshold' and non-purely military response phenomena clearly implies the application of a different

[7] See for more details: Aurel Sari, *Blurred Lines: Hybrid Threats and the Politics of International Law* (European Centre of Excellence for Countering Hybrid Threats 2018, Helsinki); Aurel Sari, 'Legal Resilience in an Era of Gray Zone Conflicts and Hybrid Threats' 1/2019 Exeter Centre for International Law Working Paper, DOI: https://doi.org/10.2139/ssrn.3315682; Aurel Sari, 'Hybrid Warfare, Law and the Fulda Gap' in Christopher Ford, Winston Williams (eds), *Complex Battle Spaces* (Oxford University Press 2019, Oxford) 161–190, DOI: https://doi.org/10.1093/oso/9780190915360.003.0006

legal regime, both in the nation-state and international context, which, if left unimproved, may even impact the legitimacy of action.[8]

In the matter of war, combatants themselves have not only sought a fire-and-brimstone approach since the beginning of history, but in order to conserve physical resources, conserve reserves and maintain high levels of capabilities before (or instead of) actual kinetic confrontations, the winning by decisive superiority without battle through deception, deterrence, the winning of hearts and minds, or the breaking of will with dominant manoeuvring has always been of great value, as Sun-tzu points out in his work The Art of War: 'supreme excellence consists in breaking the enemy's resistance without fighting'.

It took quite a long time to proceed from the less formalised use of scaremongering, propaganda, censorship and then the gradually more sophisticated and targeted use of psychology in pre-20th century conflicts to the total state control of the media in the Second World War, especially associated with the Third Reich and under Goebbels. In terms of media, the era of radio and TV, which revolutionised mass communication, was overtaken first by the explosive parallel development of telecommunications and mobile communications and then by the Internet, which by the 21st century had made entirely new forms of communication and platforms available in real-time, providing a space and a forum for communicators with a wide variety of goals, motivations and skills.

The definition and precise content of information operations are also changing and constantly evolving, and therefore, sometimes as vague or blurred as the activity itself. It follows that their classification, regulation and general analysis are also not simple and straightforward. However, in order to define the theoretical framework for this article, it is necessary to provide some relatively widely accepted starting points so that the details and specifications can be presented from common ground.

As a starting point, an accepted but somewhat understandably military-oriented definition of information operations according to NATO Policy is 'a staff function to analyze, plan, assess and integrate Information Activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and NAC approved audiences in support of Alliance mission objectives'.[9]

Cyberspace is perhaps the most dominant medium for information operations because of the extent of its use and its role in everyday life in entertainment, information, work and

---

[8] This is perfectly reflected in the issue of 'lawfare' and legal vulnerability, which makes the inadequacies and shortcomings of state regulation and competing instruments of international law an effective tool for both state and non-state actors. On the subject: Charles J. Dunlap Jr. 'Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts' <https://people.duke.edu/~pfeaver/dunlap.pdf> accessed 15 October 2024; Rode F. Kittrie *Lawfare. Law as a Weapon of War* (Oxford University Press 2016, Oxford), DOI: https://doi.org/10.1093/acprof:oso/9780190263577.001.0001; Sascha Dov Bachmann, Andres B. Munoz Mosquerra 'Lawfare and hybrid warfare – how Russia is using the law as a weapon' (2015) (102) Journal of the Society for Advanced Legal Studies 25–28, DOI: https://doi.org/10.14296/ac.v2015i102.2433

[9] NATO MC 0422 – NATO Military Policy for Information Operations, 2012. 2, <https://shorturl.at/6LTOw> accessed 15 October 2024.

access to government and commercial services. Accordingly, the academic approach has developed the concept of cyber-enabled infoops as a subcategory. According to Herbert Lin and Jackie Kerr,[10] 'information/influence warfare and manipulation (IIWAM) is the deliberate use of information by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes'.

Cognitive warfare as a new approach can be deemed a 'unification theory' concerning the matter because, as Cornelis van der Klaauw writes, 'Cognitive warfare is a structured and well[-]considered approach to target[ing] the human cognition of individuals, groups and societies in a way that affects their decision-making processes and ultimately their behaviour'.[11] This involves all means and methods, psychological or technological, that are suitable for changing the behaviour, emotion and thought processes of the targeted individual, group or population by affecting the subconscious mind. A more concentrated approach comes from Francois du Cluzel: 'the art of using technologies to alter the cognition of human targets, most often without their knowledge and consent'.[12] This definition, being narrower, clearly focuses on the technical means and the human brain as a target. To present a broader overview, we try to outline the main elements of these concepts and focus on some of the most important stages of development of the last decade.

1 NATO and Info Ops

Countering adversarial information operations, disinformation campaigns and malicious propaganda connected to diverse hybrid threats is a core allied task.[13] Article 3 of the Washington Treaty is the 'highest' point of reference and the foundation of the resilience principle, which has been of rising importance, especially since the Crimean aggression, the meddling with democratic processes and the disinformation campaigns related to the global COVID pandemic. Article 3 states: 'In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.' The Strengthened Resilience Commitment[14] in 2021 and the Strategic

[10] Herbert Lin, Jackie Kerr, 'On Cyber-Enabled Information/Influence Warfare and Manipulation' in Paul Cornish (ed), *The Oxford Handbook of Cyber Security* (Oxford University Press 2021, Oxford) 251–272, DOI: https://doi.org/10.1093/oxfordhb/9780198800682.013.15

[11] Cornelis van der Klaauw, 'Cognitive Warfare, The 21st Century Game-Changer' (2023) (39) The Three Swords 97–101.

[12] Francois du Cluzel, 'Cognitive Warfare, a Battle for the Brain' (2022) NATO ACT, STO Meeting Proceedings Paper <https://www.sto.nato.int/publications/STO%2520Meeting%2520Proceedings/STO-MP-HFM-334/%24MP-HFM-334-KN3.pdf> accessed 15 October 2024.

[13] Suzanne Waldman, Sean Havel, 'Launching Narrative into the Information Battlefield' (2022) 2 (21) Connections QJ 111–122, DOI: https://doi.org/10.11610/Connections.21.2.08

[14] NATO, Strengthened Resilience Commitment <https://www.nato.int/cps/en/natohq/official_texts_185340.htm?selectedLocale=en> accessed 15 October 2024.

Concept of 2022[15] both include marked disinformation campaigns and the coercive use of information tactics as hybrid threats, which are to be dealt with on a national and alliance level as well. Member states and the Alliance must be able to prepare for, detect, assess these and deter or defend against their use. For guidance on information operations activity areas, see paragraph 13 of MC 0422.[16]

Building upon the strategic-level alliance documents, the practical guidance on how to achieve the strategic goals is regulated on the doctrinal level. The Allied Joint Doctrine for Information Operations AJP-10.1[17] is fairly new; it was published in January 2023. The doctrine states the following ground principles for executing info ops: Comprehensive understanding, Narrative-led, Effects-focused, Integrated, Agility, Centralized planning and decentralized execution and Assessment. Information Operations staff work directly together with Strategic Communications[18] and NATO Communication Capabilities groups, namely Psychological Operations[19] and Military Public Affairs. Additional capabilities that can contribute to an info ops campaign are cyberspace operations, electromagnetic warfare, civil-military cooperation, physical destruction (kinetic force), operations security and deception, information assurance and emerging and disruptive technologies.

An overview of the above elements is necessary for assessing the principles, approaches and tools that may emerge in the context of info ops, whether defensive or active. It is also important to assess our own theoretical frameworks, thus creating a basis for comparison with the ideas of our counterparts and for outside-the-box innovations that may emerge.

2 Information/Influence Warfare and Manipulation

Herbert Lin's term was developed to describe the rising importance of information warfare as a form of confrontation to which liberal democracies are particularly vulnerable and are not particularly potent compared to usually authoritarian adversaries who specialise in this form of conflict and use free speech and freedom of ideas as a weakness. Lin also pointed out

15 NATO, NATO 2022 Strategic Concept <https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf> accessed 15 October 2024.

16 NATO MC 0422 2012.

17 AJP-10.1, 26.

18 Military Committee (MC) 0628, NATO Military Policy on Strategic Communications: 'in the NATO military context, the integration of communication capabilities and the information staff function with other military activities, in order to understand and shape the information environment, in support of NATO strategic aims and objectives'.

19 Allied Joint Publication (AJP)-3.10.1, Allied Joint Doctrine for Psychological 2 AJP-10.1 31 Edition A Version 1 + UK national elements Operations and MC 0402, NATO Military Policy on Psychological Operations: 'planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives'.

the doctrinal confusion in an article[20] in 2020. Reference to 'Information Warfare' appeared first in 1992 in a US Department of Defense (DOD) directive and later in 1996 in a doctrine. This changed to 'Information Operations' in 1998. Influence Operations was not a DOD term; it appeared in a study by the RAND Corporation in 2009. Psychological operations are a key component of information operations, but this has a deeper history. Last, the concept of 'Cyberspace Operations' was introduced in 2013. All these involve very similar key components and important overlaps, not just from the public viewpoint but in terms of political leadership and other military and defence functions. As Lin states,[21] 'Using these same terms differently in different contexts is likely to create conceptual confusion that in turn can also result in [the] misallocation and misalignment of resources and capabilities.'

3 Cognitive Warfare

As a next evolutionary step, NATO is developing the idea of Cognitive Warfare. Leading researchers Bernard Claverie and Francois du Cluzel have published many papers[22] on this new concept, going as far as to claim that human cognition is the sixth domain of warfare (after land, sea, air, space and cyber). With rapid advances in the fields of nanotechnology, biotechnology, information technology and cognitive sciences, the misuse of knowledge about the functions of the human brain is a rapidly growing risk. It brings with it a new (third) dimension of warfare, the cognitive space, in addition to the physical and informational.

The development of the new concept is such a major objective that the First NATO scientific meeting on Cognitive Warfare was held in France in June 2021.

4 Some Thoughts About Cyber Sovereignty

The legal assessment of sovereignty is not only closely linked to cyberspace operations in the narrow sense but also to information and cognitive warfare; since the primary tool and theatre of these operations in the 21st century is cyberspace, it is clear that the issue of sovereignty is also of vital importance for states in their own national information spaces.

Sovereignty is an ancient legal principle aligned with territoriality that guarantees peaceful coexistence through mutual recognition between states.[23] In modern international

---

[20] Herbert Lin, 'Doctrinal Confusion and Cultural Dysfunction in DoD Regarding Information Operations, Cyber Operations, and Related Concepts' (2020) 5 (2) The Cyber Defense Review 89–108.

[21] Lin (n 20) 100.

[22] Bernard Claverie, Francois du Cluzel, 'The Cognitive Warfare Concept' (2023) NATO ACT <https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf> accessed 15 October 2024.

[23] Dieter Grimm, *Sovereignty – The Origin and Future of a Political and Legal Concept* (Columbia University Press 2015); Lucie Kadlecová, *Cyber Sovereignty – The Future of Governance in Cyberspace* (Stanford University Press 2024).

law, the definition set out in the *Las Palmas Case* of 1928[24] is taken as the authoritative one: '[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.' The state has the capacity to exercise power independently inside its borders; in relations extending outside the state, nations have the right to self-determination and to act without external coercion and international law respects this.

Over the past millennia, this approach has helped establish the jurisdiction of states involved in a given matter in a significant number of cases and determine the legal status of parties in a given situation. However, in cyberspace, the cross-border services and the technical solutions that allow anonymity make it far from easy to apply this principle and, in some cases, to enforce and recognise it,[25] even though sovereignty as a core principle has been considered valid in relation to cyberspace by several international organisations and national declarations on the legal regime applicable to cyberspace.

Although Hungary has not yet issued a comprehensive national position[26] on the legal framework for cyberspace, the concept is reflected in several strategies and laws. The legal definition of cyberspace in Hungary is currently: 'the part of the electronic information systems of the global cyberspace that are located in Hungary and the social and economic processes that take place in Hungary or are directed to Hungary or involve Hungary, which are represented by data and information through the electronic systems of the global cyberspace'.[27] Obviously, at least four or five elements of this sentence may overlap with other states' similar national definitions of cyberspace, especially since there are several competing approaches to the interpretation of the violation of sovereignty in cyberspace.

The more defensive view is that its violation is a breach of a substantive primary rule of international law and constitutes an internationally wrongful act. Regarding the more permissive approach, sovereignty is merely a principle of international law; cyber operations cannot violate sovereignty as a rule of international law, although they may constitute prohibited interventions, use of force or other internationally wrongful acts.

According to the assessment prevailing in NATO member- and friendly states, the principles of international conventions, customary law and customary international law remain valid and applicable in cyberspace. The Tallinn Manual,[28] which contains five main rules for the interpretation of sovereignty in cyberspace, is the practical embodiment and

---

[24] *Island of Palmas Case* (United States v The Netherlands), Permanent Court of Arbitration, 2 U.N. Reports of International Arbitral Awards 829 (1928).

[25] Gergely Gosztonyi, *Censorship from Plato to Social Media. The Complexity of Social Media's Content Regulation and Moderation Practices* (Springer 2023, Cham) 157–165, DOI: https://doi.org/10.1007/978-3-031-46529-1_11

[26] For national positions, see <https://cyberlaw.ccdcoe.org/wiki/Sovereignty#cite_note-1> accessed 15 October 2024.

[27] Act 50 of 2013 on electronic information security in public and local government bodies, § 1(1)35.

[28] Michael N. Schmitt (ed), *Tallinn Manual 2.0,* (Cambridge University Press 2017, Cambridge) DOI: https://doi.org/10.1017/9781316822524

professional guide to this. Using another approach, a new set of international conventions based on international consensus that respects existing international legal rules and goes beyond multiple interpretations based on analogies could indeed be a forward-looking and useful solution to the legal problems of cyberspace. Preparatory work on this has been ongoing for some time in the framework of the UN Open-Ended Working Group on Information and Communication Technologies (OEWG), which currently has a mandate until 2025. However, increasing multipolar competition is also present in the OEWG, and national positions are far from converging.[29]

According to Aleksi Kajander,[30] the principle of sovereignty and its implications for cyberspace remained a contested issue in the sessions in 2023, and the publishing of detailed national positions on international law and cyberspace, which was encouraged by numerous states at the OEWG, is a crucial step towards creating a common understanding of how pre-existing international law applies in cyberspace and what gaps exist because recognition of the existence of state positions reduces the possibility of unfounded claims based on 'majority positions'.

The growing threats in cyberspace, which are in no small part directly or indirectly attributable to state actors, also have negative effects on global production and trade. It is not surprising that economic operators and the key companies in the tech sector that are primarily affected are also calling for a more secure environment. A good example is Microsoft's Digital Geneva Convention initiative, which encourages states' efforts to strengthen international cybersecurity standards, create new binding rules and protect civilians, similar to the Geneva Conventions.[31]

The tech sector's perspective is relevant because their influence, operation and impact in cyberspace are at least on a level with, and sometimes even above, that of the nation-states that legislate. The phenomenon of techno-polarity[32] describes this opposition, where the arena of competition is cyberspace, data traffic, algorithms and cloud and server environments, not physical space and territory. With the decentralised operations in the cloud, blockchain technology and the possibility of anonymisation, the abuse of AI

[29] Sean S. Costigan, 'Sovereign or Global Internet? Russia and China Press for Cybercrime Treaty' (2021) 20 (2) Connections QJ 9–13, DOI: https://doi.org/10.11610/Connections.20.2.01; Creemers R.J.E.H., 'China's conception of cyber sovereignty: rhetoric and realization' in Dennis Broeders, Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy. Digital Technologies and Global Politics* (Rowman & Littlefield, 2020) 107–142, DOI: https://doi.org/10.2139/ssrn.3532421

[30] Aleksi Kajander, *A Tale of Two Draft Resolutions: A Report on the Polarising International Law Discussions at the 2023 OEWG Substantive Sessions* (NATO CCDCOE 2023, Tallinn).

[31] Brad Smith, 'The need for a Digital Geneva Convention' (14 February 2017) Microsoft Blog <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention> accessed 15 October 2024.

[32] N/A, 'Cyber Sovereignty' Synergia Foundation, 27 April 2024, <https://www.synergiafoundation.org/insights/analyses-assessments/cyber-sovereignty>

developments may further reduce trust between parties, which may lead to strategies for sourcing from trusted sources that limit free market operations.[33]

Another important issue related to cyber sovereignty in the context of information operations is net neutrality, which directly affects freedom of expression and freedom of information, with proponents arguing for the non-discrimination of network traffic and opponents arguing for security interests from a public perspective and commercial interests from an economic one.[34] The US approach, with its dominant influence over the operation of the Internet, is clearly dominant globally, and it is important to be alert to the decisions taken by the Federal Communications Commission (FCC), the courts and the legislature in favour of net neutrality, which is more likely to be supported under Democratic leadership.[35]

5 A Proposal for Regulating Info Ops

The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities[36] can be identified as an international legal professional initiative comparable to the Tallinn Manual. This initiative by the Oxford Institute for Ethics, Law and Armed Conflict aims to establish a 'no-go' list for information operations in the context of human rights protection. The main guidelines set out in the ten rules are that States must refrain from violating the principles of sovereignty and non-intervention and from any propaganda that promotes war, national, racial or religious hatred and discrimination. They must enforce these in their jurisdictions and also refrain from activities that violate the fundamental human rights of individuals within their jurisdiction (including the freedom to seek, receive and impart information).

States must take measures to protect the human rights of individuals within their jurisdiction from violation by information operations. Protective measures should have a legitimate purpose, legality, necessity, and proportionality and not involve discrimination. The regulation of info ops must not unduly restrict human rights, and states must ensure that information and technology companies are able to operate their services consistently in accordance with the human rights of their individual users.

---

33 N/A, 'Cybersecurity in the EU – Member State Implementation of the NIS2 Directive: The Example of the Czech Republic' (July 2023) Morgan Lewis Report 10.

34 Christian Hildebrandt, Lukas Wiewiorra, 'The past, present, and future of (net) neutrality: A state of knowledge review and research agenda' (2024) 39 (1) Journal of Information Technology 167–193, DOI: https://doi.org/10.1177/02683962231170891

35 Tom Wheeler, 'Don't be fooled: Net neutrality is about more than just blocking and throttling' (30 October 2023) Brookings, <https://www.brookings.edu/articles/dont-be-fooled-net-neutrality-is-about-more-than-just-blocking-and-throttling> accessed 15 October 2024.

36 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities' <https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities> accessed 15 October 2024.

The conduct of information operations or activities during armed conflict is subject to the applicable rules of international humanitarian law; it prohibits engaging in information operations or activities that amount to international crimes, such as genocide, including direct and public incitement thereto, war crimes and crimes against humanity.

III Links between Legal Response Options and Resilience

Given the highly complex social, psychological, technological, political, economic and, through them, security implications of the development of info-communications, it is not historically surprising that state and non-state actors alike are seeking to use the achievements associated with this development to advance their own interests *vis-à-vis* others. This leads to a number of novel phenomena ranging from the rivalries of global capitalism to great power competition and crime.[37]

In a changing environment, states, as the organisational system that ensures the orderly coexistence of individuals and their societies, must adapt to change. This implies the development of rules concerning both passive (defensive) and active (advocacy/preventive) state capacities, structures and, in the case of states obeying the rule of law, legal systems. Moreover, this environmental change also sheds new light on the state's self-understanding and the question of sovereignty. Indeed, security awareness, security self-consciousness and consent to state action on the part of individuals and society are essential for effective defence and advocacy in large-scale, networked systems with a high degree of freedom. This can only be guaranteed if resilience is strengthened by treating the state-society system as a whole and by promoting and supporting the security-enhancing potential and awareness of individuals.[38] It is important to stress, however, that without predictable security, individual, social, political and economic confidence is undermined; creative, innovative and productive capacity is reduced, and, ultimately, the degree of freedom is also reduced, which is a clear loss for society as a whole.

It is no coincidence that in many successful model states (such as Switzerland or even Singapore), social and economic productivity is clearly linked to an effective defence-security system and the strengthening of security awareness is based on state and social cooperation. The Nordic and Baltic states' efforts to strengthen security through social cooperation are a similar example.[39] The developmental orientation of NATO and the EU

[37] Benoît Dupont, Thomas Holt, 'The Human Factor of Cybercrime' (2022) 40 (4) Social Science Computer Review 860–864, DOI: https://doi.org/10.1177/08944393211011584

[38] See, for more details: Inez Miyamoto, 'Disinformation: Policy Responses to Building Citizen Resiliency' (2021) 20 (2) Connections QJ 47–55, DOI: https://doi.org/10.11610/Connections.20.2.05; Jim Townsend, Anca Agachi, 'Build Resilience for an Era of Schocks' in Christopher Skabula (ed), *NATO 20/2020. Twenty Bold Ideas to Reimagine the Alliance after the 2020 US Election* (The Atlantic Council 2020, Washington DC).

[39] See, for example: Ieva Bérzina, 'Total defence as a comprehensive approach to national security' in Nora Vanaga, Toms Rostoks (eds), *Deterring Russia in Europe. Defence Strategies for Neighbouring States* (Routledge

(such as the recent legislative results, NIS2 and CER Directives, and the DORA Regulation) in recent years also reflects this trend.

The overall development of information technology, but also of the public services – critical infrastructure – based on the former that underpin the development of a welfare/consumer society, and their becoming a basic necessity has clearly created an extensive, complex, networked and thus multipolar and multi-exposed system in which security cannot be guaranteed by the state alone, at least not without adequate social support, attitudes and security awareness. To think that security can be maintained in this environment by purely state means, by acting 'above' society, is an illusion. However, the idea of self-organisation and self-education at the individual and societal levels that would trigger state action on the grounds that the digital space available to all is also an unrivalled knowledge and organisational base seems equally utopian.

In light of this, we believe that the solution to the challenge lies between the two extremes, where we accept and acknowledge that self-education, self-organisation and security awareness at individual and societal levels have become key but accept and support the modernisation of state capabilities and socio-state cooperation to increase their effectiveness. This could be the real basis for resilience, where – from education and training to the functioning of public administration and defence and security activities – efforts are made to go beyond rigid state-society demarcation in the field of resilience through cooperation.

Resilience has great potential, as it is not only a means of defending oneself but also of defending oneself as an individual, a society and a state. Effectively building resilience also means developing the necessary user, productive, innovative, theoretical-scientific and practical capacities that can boost social and public productivity and security.

However, this requires accepting that the idea, areas and strengthening of resilience must be gradually built into the public and regulatory space and enhanced in the social dimension through the resources and support potential that this offers. This requires:

1. Credible analyses and assessments of related environmental changes and challenges.
2. The credible, well-founded and effective modernisation of public institutions and regulations.
3. Authentic information and communication about security[40] to be separated and compartmentalised as much as possible from domestic and international political competition.
4. Supporting, without controlling, self-organising efforts to promote self-education and security awareness at individual and societal levels.

2019, Abingdon) 71–89, DOI: https://doi.org/10.4324/9781351250641-5; James Kennet Wither, 'Back to the future? Nordic total defence concepts' (2020) 20 (1) Defence Studies 61–81, DOI: https://doi.org/10.1080/14702436.2020.1718498

40 Cullen G. Nutt, Reid B.C. Pauly, 'Caught Red-Handed: How States Wield Proof to Coerce Wrongdoers' (2021) 46 (2) International Security 7–50, DOI: https://doi.org/10.1162/isec_a_00421

5. Increased support for innovations that strengthen resilience.
6. Stepping up education and training programmes, supervised and organised by the state, but with ongoing social consultation.

Such an approach clearly shows that resilience-building can be approached from at least two angles. The first is associated with NATO's now traditional territorial division.[41] The second is the division into the relevant disciplinary/action dimensions. However, the second approach is also crucial for the effective development, operation and maintenance of the areas of action defined by NATO since it can overcome the *prima facie* obvious but erroneous view that all this can be guaranteed by the state's capabilities, primarily in the areas of defence and related state administration.

The areas of resilience are all those in which social actors are present as both professionals and users/actors. The former's effective provision cannot, therefore, be limited 'only' to the staff (and their awareness) in the public service or the sectors that provide the services in question. In one way or another, society as a whole is directly and indirectly involved through supply chains, public services and the daily activities necessary for a well-ordered life.

Therefore, a key issue for effective development in these areas of resilience is the strengthening of a supportive social environment, which involves education and training, professional cultures/chambers of commerce/training centres, research and development and the sphere of civil society organisations as intermediary environments. In addition, providing and updating the professional and public-regulatory framework within which these areas operate is a perspective that extends beyond the state, as is promoting a social understanding of the anomalies that exist in certain areas based on abuses for the purpose of promoting order and efficiency in society as a whole. In this context, enhancing resilience is therefore not only a task and challenge for the whole of government – ie one that should take effect across the professional-sectoral divide within government – but also for society as a whole, for which the state can provide a framework, targeted support and credible basic information that is acceptable to society at certain points, while only at other points can it be the sole or primary custodian of active action through its defence and security agencies.

IV Closing Thoughts

Our review of the interpretation, doctrinal background and regulatory issues related to information operations, as well as our focus on cyber sovereignty, has, we believe, established our hypothesis that information operations pose significant regulatory challenges and require systemic renewal in response.

[41] NATO, Resilience, civil preparedness and Article 3 <https://www.nato.int/cps/en/natohq/topics_132722.htm> accessed 15 October 2024.

International attempts to develop positive legal definitions with a view to unifying and defining them are not capable of producing results at the global level in the medium term, given the geostrategic shift towards multipolarity, but this does not mean that efforts at the alliance, EU and national levels to do so are negligible. Moreover, without a clear national position, the national interest cannot be consistently and clearly represented at the international level, and the loss of alliance confidence and credibility in the balance of national security interests must be assessed against sometimes useful ambiguity at the strategic level.

It is self-evident that with such a broad impact mechanism or, rather, matrix, security factors and, to a considerable extent, military aspects will also be present. Clearly, the information space has led to revolutionary developments in non-kinetic modes of warfare, the full horizon of which is perhaps not yet fully appreciated, especially if we look beyond the concept of warfare, which in many respects is considered restrictive, to the whole concept of complex security.[42]

However, it must also be recognised that the information space, and with it, information society, is so multifaceted and complex that its study can only be properly grasped as an intersection of many disciplines and scientific fields. Accordingly, we perceived it as important to take a similar approach in this paper to the interconnections of the information age, particularly concerning the defence and security aspects of the state, paying attention to constitutional, sociological and, to some extent, governance aspects, in addition to the perhaps traditional military/war science approaches.[43]

Perhaps the most striking novelty of the information age is the unprecedented importance of the social milieu in guaranteeing security while the traditional functions of the state are maintained. It should be stressed that the social environment has always been important in warfare and the broader guarantee of order and security, but the technological changes of our time and their natural infiltration into the fabric of society make it difficult or impossible to imagine a security system with a 'state only' or 'social only' emphasis. From this perspective, the information age and information society should, therefore, entail not only the modernisation, networking and complexification of the defence and security structures, instruments and rules of the state but also a significant strengthening of national resilience.

In the context of a mostly legal but multi-disciplinary analysis of information operations, our main proposal is, therefore, to identify possible regulatory directions and to pursue a comprehensive approach while embedding this issue within the framework of resilience. Indeed, the states and societies of the information age interact so closely in the cognitive dimension that it is only in this complex space that the development of appropriate new frameworks and solutions can be properly understood.

---

[42] Risa Brooks, 'Paradoxes of Professionalism: Rethinking Civil-Military Relations in the United States' (2020) 44 (4) International Security 7–44, DOI: https://doi.org/10.1162/ISEC_a_00374

[43] Rachel Tecott Metz, Andrew Halterman, 'The Case for Campaign Analysis: A Method for Studying Military Operations' (2021) 45 (4) International Security 44–83, DOI: https://doi.org/10.1162/isec_a_00408

ELTE LAW JOURNAL

CONTENTS