7 Cyberespionage and human rights: A disappointing balance

Sophie Duroy and Liliya Khasanova

7.1 Introduction

The status of cyberespionage in international law raises many questions. Cyberespionage has the potential to seriously affect the economic, political, and social life of targeted states, but most states are unable to stay up to date with the technological developments needed to detect and prevent unwelcome intrusions. This factual situation has heightened the need to identify a legal framework that could limit state-sponsored cyberespionage, triggering discussions on how peacetime cyberespionage fits into the existing international law framework, and in particular with the principle of sovereignty.[1] Less discussed is the status of cyberespionage with regard to individuals' rights.[2] This matter is, however, crucial. Individuals can be the direct target of cyberespionage, which then tends to be called (electronic) (mass) "surveillance", but they may also be collateral to untargeted or state-targeted cyberespionage. With individuals being potentially affected by all cyberespionage practices, it becomes critical to assess whether existing human rights frameworks have the potential to curtail ever-expanding practices of cyberespionage. Should it be so, states' security against cyberespionage would also be enhanced. Indeed, the best way to guarantee widespread cybersecurity to both states and individuals in the context of cyberespionage would be to ensure that cyberespionage is conducted

1 E.g., Dapo Akande, Antonio Coco, and Talita de Souza Dias, 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies' (2022) 99 International Law Studies; Russell Buchan, *Cyber Espionage and International Law* (Hart Publishing 2019); François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020); Harriet Moynihan, 'The Application of International Law to State Cyberattacks' (2019) Chatham House Research Papers; Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2021); Antonio Coco, Talita Dias, and Tsvetelina van Benthem, 'Illegal: The SolarWinds Hack under International Law' (2022) 33 European Journal of International Law 1275. Kristen E. Eichensehr, 'Not Illegal: The SolarWinds Incident and International Law' (2022) 33 European Journal of International Law 1263.

2 For scholarly engagement with this question, see: Eliza Watt, *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law* (Edward Elgar Publishing 2021); Buchan (n 1). The SURVEILLE project also partly focused on the impact of mass surveillance on human rights (SURVEILLE 'Surveillance: Ethical issues, legal limitations, and efficiency' FP7-SEC-2011-284725).

DOI: 10.4324/9781003344124-7

with full respect for international human rights law (IHRL), regardless of whether individuals constitute the direct target or are collateral. Yet, it is anything but certain that human rights are adequately protected against cyberespionage under current frameworks, and even less certain that these frameworks can effectively curtail increasingly intrusive practices of cyberespionage.

Let us first go back one step, and explain the relevance and role of IHRL in the governance of cyberespionage. Intelligence practices such as cyberespionage epitomize the liberty-security conundrum.[3] That is, they exemplify a purported necessity to trade some amount of liberty or rights in exchange for heightened security. Surveillance, for instance, notoriously infringes on individuals' right to privacy. States' rationale for surveillance practices is that a phenomenon (terrorism; organized crime) represents a threat to a legitimate interest, such as national security or public order. According to states' justifications, this threat's existence necessitates a response to prevent it from materializing: surveillance. Hence, to protect national security against terrorism or organized crime, citizens need to accept that they will have less privacy.[4] This trade-off seems intuitive and states present it as unavoidable. However, this reliance on a balancing or trade-off between security and liberty is subject to many fallacies. As the Pegasus scandal demonstrated, providing the state with the means to fight our common enemies also (and often mostly) allows it to fight its own enemies.[5] The Snowden leaks showed that, in this respect, mass surveillance is subject to the same deviances as targeted surveillance.[6] Further, as the multidisciplinary SURVEILLE project highlighted, electronic mass surveillance produces at best medium-level usability scores (i.e., it is not very useful in detecting threats), while triggering extremely high intrusion on the right to privacy.[7] This means that the price to be paid in terms of the reduction in rights is grossly disproportionate to the potential security gains. Moreover, with mass surveillance, it becomes clear that the sacrifice of both privacy rights and the

3 The following two paragraphs draw on the argument one of us made in: Sophie Duroy, *The Regulation of Intelligence Activities under International Law* (Edward Elgar Publishing 2023) Chapter 1.

4 Notwithstanding that non-citizens and/or non-residents generally have no choice but to accept this trade-off in which their security is often not part of the deal.

5 Pegasus is spyware developed and commercialized to states by the Israeli company NSO. Pegasus can be covertly installed on most mobile devices and has been used by many governments against opposition figures, journalists, and human rights activists, among others. See, e.g., the Guardian's Pegasus homepage for news and explainers: https://www.theguardian.com/news/series/pegasus-project. For a legal assessment, see Giovanni Sartor and Andrea Loreggia 'The impact of Pegasus on fundamental rights and democratic processes' European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies PE 740.514 - January 2023.

6 For a catalog of the various revelations by Edward Snowden regarding the United States' surveillance activities, see Lawfare, 'Snowden Revelations': https://www.lawfareblog.com/snowden-revelations.

7 SURVEILLE 'Surveillance: Ethical issues, legal limitations, and efficiency' FP7-SEC-2011-284725. See Deliverable D2.8: SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act; SURVEILLE Paper on Mass Surveillance by the National Security Agency (NSA) of the United States of America. For more information on the project, see: https://surveille.eui.eu/.

rule of law affects everyone – not just the terrorists, criminals, or those we consider "others".

Cyberespionage is thus rationalized by the alleged necessity of balancing liberty and security. However, human rights are on both sides of the equation. Security is not an abstract value. When we speak of security, whether individual or national, we speak of the security of our rights – as individuals and as a community. We value national security not in its own right but because it is a necessary part of protecting individual and collective rights.[8] In turn, as Ross Bellaby argues, the (ethical) value of espionage comes from its role in protecting the individual and the political community.[9] In consequence, because human rights are on both sides of the liberty-security equation, the permissibility of espionage activities infringing on human rights should be assessed from a human rights perspective.

International human rights law constitutes a self-contained system of norms complete in itself, in the sense that it comprises the necessary rules and procedures to assess whether an infringement on a right constitutes a violation thereof or is instead justified by competing interests. Indeed, permissible exceptions to the norm, restrictions upon rights, and circumstances precluding wrongfulness are all provided by the legal framework itself. The consequence is that legal norms are not to be balanced against extra-legal considerations, as the liberty-security conundrum implies. Rather, competing interests are balanced through legal norms and mechanisms. In its current form, the international human rights framework is thus flexible enough to provide states with all the necessary means and methods to protect their political communities and individuals while respecting states' common values (as reflected in international law), including and especially in times of acute crisis. The IHRL framework thus applies to states' cyberespionage practices whenever they infringe on human rights.

In this Chapter, we assess the potential of human rights to curtail cyberespionage practices. We first assess law-making efforts in multilateral settings, reviewing efforts to regulate state-sponsored operations in cyberspace, including cyberespionage, and the role that human rights norms have played in such norm-making endeavors (Section 7.2). Concluding that a binding multilateral treaty regulating malicious cyber operations or cyberespionage specifically is extremely unlikely to be adopted in the near future, we move on to assessing the potential of human rights courts and bodies to curtail ever-expanding practices of electronic mass surveillance and indiscriminate data retention (Section 7.3). This section focuses especially on the case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), which remain the only supra-national courts to have directly assessed states' cyberespionage practices against IHRL. We argue that, despite procedural adaptations to cyberespionage and a promising early case law, European human rights courts have ultimately failed to mobilize the human

8 Jeremy Waldron, *Torture, Terror, and Trade-Offs: Philosophy for the White House* (Oxford University Press 2010) 116.

9 Bellaby (n 3) 4.

rights framework to meaningfully curtail cyberespionage, instead succumbing to a balancing act favoring states' national security arguments. In a final section, we outline the consequences of law-making failures and of European courts' principled acceptance of mass surveillance and indiscriminate data retention for future developments (Section 7.4).

7.2 Multilateral developments

At the moment, there is neither political will and trust, nor effective negotiation forums that could facilitate the regulation of peacetime cyberespionage and limit its infringement on human rights on a multilateral level. Generally, a strong divergence in the process and substance of international norm-making in the field of cybersecurity makes an agreement on binding norms curtailing state-sponsored espionage very unlikely (7.2.1). Furthermore, the push for a human rights-centered approach to cybersecurity is also experiencing strong resistance on a multilateral level (7.2.2).

7.2.1. The improbability of a multilateral cyber agreement

Information and communication technologies (ICTs) have opened new dimensions and possibilities for intelligence operations. The resulting facilitation of data collection and analysis methods leads to a potentially unlimited reach of cyber operations. States' willingness to regulate activities in cyberspace has been amplified by these extended technical capabilities, by operations' anonymous, instantaneous, and a-territorial character, and by the significant role of private actors in conducting them. The Snowden revelations (2013), the SolarWinds hack (2020),[10] cyber electoral interference, and economic cyberespionage have elevated states' interest in finding a common understanding of *how* international law applies in cyberspace. At the same time, this series of malicious activities has undermined trust between both rivals and allies, leading to a growing number of law-making initiatives to enhance resilience at a national and regional (rather than multilateral) level.

While embracing multilateral efforts to develop norms of responsible state behavior in cyberspace and committing to confidence-building measures, states emphasize the centrality of defensive cybersecurity and the importance of independent cyber resilience. This rise of neo-sovereignty, even in a domain that is *a priori* a-territorial and a-material,[11] as well as different perceptions of the role and scope of the international rule of law in cyberspace, have complicated the process of norm creation and implementation on a multilateral level. Agreeing on a set of binding rules seems especially difficult in the current geopolitical climate.

10 See Coco, Dias, and van Benthem (n 1).

11 Nicholas Tsagourias, 'The Rule of Law in Cyberspace: A Hybrid and Networked Concept?' (2020) 80 (2) Heidelberg Journal of International Law 433.

One of the functional attributes of international law is the creation of a framework of institutions and practices through which states can create substantive rules and mediate clashes of interests and conflicting values.[12] The issue of information security has been on the UN agenda since 1998.[13] Several years of successful discussions in the Group of Governmental Experts (GGE)[14] led to the recognition of the applicability of existing international law to states' cyber activities in 2013.[15] The 2015 report of the Group,[16] in contrast, reflected the deeply diverging views of the 20 participants on cornerstone issues related to attribution, self-defense, international humanitarian law, and human rights. The report of 2017 was not adopted at all.[17]

In 2018, the divide in positions escalated further when, as a pushback to the GGE, Russia introduced a UN General Assembly (UNGA) Resolution that established a new working group under UN auspices: the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG). The differences between the GGE and OEWG processes lay mostly in the nature and number of stakeholders included in the discussion: the latter includes all the UNGA members as well as non-governmental actors, as compared to the GGE's experts, who come from 25 States and work in their personal capacity.[18] During the same 2018 session, the US introduced a resolution establishing another GGE,[19] meaning that parallel work in two forums continued until each group adopted a report in 2021.[20] Although the last mandate of the GGE was not renewed, the confrontation persists as the Program of Action (PoA) – a

12 Andrew Hurrell, 'International Law and the Changing Constitution of International Society' in Michael Byers (ed), *The Role of Law in International Politics: Essays in International Relations and International Law* (Oxford University Press 2001).

13 The agenda was initiated by Russia in 1998. See the first resolution of the UNGA: A/RES/53/70 on Developments in the field of information and telecommunications in the context of international security (1998).

14 The UN Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security was established by the UNGA in 2004 to examine the impact of the developments in ICT on national security and military affairs. It was composed of 20 (later 25) members based on equitable geographical distribution and included five permanent members of the UN Security Council.

15 UN GA (2013) UN Doc A/RES/68/98.

16 UN GA (2015) UN Doc A/RES/70/174.

17 Elaine Korzak, 'UN GGE on Cybersecurity: The End of an Era?' (*The Diplomat,* July 31, 2017) <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/> accessed 27 November 2022.

18 UN GA Resolution 'Developments in the field of information and telecommunications in the context of international security' (2018) UN Doc A/RES/73/27.

19 UN GA Resolution 'Advancing responsible state behavior in cyberspace in the context of international security' (2018) UN Doc A/RES/73/266.

20 UN GA (July 14, 2021) UN Doc A/RES/76/135; UNGA 'Open-ended working group on developments in the field of information and telecommunications in the context of international security' (March 10, 2021) UN Doc A/AC.290/2021/CRP.2.

proposal initiated by France and Egypt in 2020 – introduced another alternative to the OEWG negotiation format.[21]

The PoA amplifies several new levels of disagreement related to global governance in cyberspace. First, the like-minded states behind the PoA are reluctant to further negotiate binding norms and, in particular, the adoption of a multilateral treaty. Instead, these states seek to discuss and agree on a set of voluntary norms to regulate state activities in cyberspace, mainly focused on implementing existing recommendations, norms, and principles.[22] Meanwhile, Russia and China, supported by the majority of the members of the Shanghai Cooperation Organization (SCO), continue to insist on the importance of a multilateral treaty in all of their statements and initiatives.[23]

Secondly, the increased participation of non-state actors in the norm-making process triggers tensions among states. Private companies and non-governmental organizations play a significant role in the evolution[24] and implementation[25] of cyber norms. The OEWG thus includes a wide range of non-governmental organizations and tech companies that consult and provide input for the discussions of the reports. Despite this extended membership, the process remains very state-centric and political. While most Western states strongly endorse the "multi-stakeholder" approach, China and Russia expressly support the competing "multilateral", state-centric conception of cyberspace governance.[26] Amidst geopolitical disputes, the deepening cleavages between Western states and Russia and China heavily influence the participation of certain stakeholders in meetings. In July 2022, at the beginning of the new OEWG round of negotiations, twenty-two international NGOs and several Russian organizations had their accreditation blocked for the current OEWG mandate period by Russia and Ukraine, respectively.

The various international negotiation forums on cybersecurity exemplify a wide divergence in states' visions for the permanent institutional framework and practice of norms and rulemaking in cyberspace, not to mention differences in their approaches to the substantive interpretation and application of international legal norms. In such circumstances of ideological confrontation and, given the willingness of major players to control the agenda, the adoption of a multilateral

21 Fifty-three states are co-sponsoring the establishment of a UN PoA as a "permanent, inclusive, consensus-based and action-oriented format" to advance responsible behavior in the use of ICTs in the context of international security. The official text of the proposal is available at: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf.

22 Delerue (n. 1) 25.

23 'Convention on International Information Security' (The Ministry of Foreign Affairs of the Russian Federation, 22 September 2011).

24 Tsagourias (n 11).

25 Sheetal Kumar, 'The Missing Piece in Human-Centric Approaches to Cybernorms Implementation: The Role of Civil Society' (2021) 6 Journal of Cyber Policy 375.

26 Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development (February 4, 2022) <http://en.kremlin.ru/supplement/5770> accessed 27 November 2022.

agreement outlining states' responsibility for malicious cyber operations seems very unlikely.[27] This leads us to explore the question of whether a special agreement on the regulation of and limits to peacetime cyberespionage activities is possible.

The subject of peacetime cyberespionage is traditionally avoided in multilateral settings.[28] Espionage lacks an internationally recognized normative definition,[29] and the matter does not get clearer with *cyber* espionage. International law does not regulate peacetime espionage *per se*. However, the application of international law to peacetime cyberespionage has been thoroughly studied in recent years, predominantly by Western scholars.[30]

The Tallinn Manual 2.0 highlights that "although peacetime cyber espionage by States does not per se violate international law, the *method* by which it is carried out might so".[31] Further, a growing number of states adopt a defensive position towards cyberespionage and follow a "sovereignty as a rule" approach, stating that any intrusion into the work of ICT located on their territory (irrespective of the seriousness of the effects) would be a violation of their sovereignty.[32] Thus, the absence of *lex specialis* rules concerning (cyber) espionage does not necessarily mean that it is internationally lawful, nor that it should be.

Notwithstanding states' understanding of the vulnerabilities associated with state-sponsored cyberespionage and their interest in constraining it, it seems unlikely that these practices will be directly restricted by binding norms on a multilateral level. The Council of Europe's Intelligence Codex, which attempted to introduce a prohibition on political and economic espionage, was rejected in 2015.[33] This was the case despite a favorable geopolitical context in the direct aftermath of the Snowden revelations. As we explain in the following section, other attempts to introduce voluntary normative restrictions under the human rights framework in the UN were equally fruitless.

27 Watt (n 2) Conclusions.

28 On a bilateral level, there was an agreement between China and the US on preventing economic cyberespionage, however, it is also not clear how effective it was in terms of malicious operations and establishment of trust.

29 For some scholarly attempts at defining 'intelligence', see for instance Michael Warner, 'Wanted: A Definition of "Intelligence"' (2002) 46 Studies in Intelligence 9; Peter Gill and Mark Phythian, *Intelligence in an Insecure World* (Wiley 2012) 19.

30 For more on international law and cyberespionage, see: Watt (n 2); Buchan (n 1); Duroy (n 3). Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, 2nd ed. (Cambridge: Cambridge University Press, 2017); Oğuz Kaan Pehlivan. *Confronting Cyberespionage under International Law.* Routledge, 2019.

31 Tallinn Manual 2.0 (n 30), Rule 32 (emphasis added).

32 Among these countries are Germany, France, Canada, Netherlands, New Zealand, Chile, Bolivia, Guatemala, and Guyana.

33 CoE, Committee on Legal Affairs and Human Rights, 'Mass Surveillance. Draft Resolution' (2015) AS/Jur 2.

7.2.2. Human rights' struggles in cyber negotiations

Not only did Edward Snowden's revelations impact trust between allies and raise cybersecurity concerns, they also uncovered the threats that mass cyber surveillance poses to individual rights. Until cyber operations opened the possibility of conducting surveillance that could affect virtually everyone, public pressure to protect citizens from espionage was minimal. In the aftermath of the Snowden disclosures, however, states have been tasked with finding a balance between protecting human rights and enjoying the potential national security benefits of mass cyber surveillance.

In response to the exposed NSA mass surveillance programs, Germany and Brazil introduced a draft resolution in the UNGA that envisaged the extraterritorial applicability of the right to privacy in surveillance activities.[34] Unsurprisingly, such extraterritoriality was objected to by the US.[35] Notwithstanding, the compromised final Resolution on the Right to Privacy in the Digital Age was adopted by consensus in the UNGA and included the crucial statement that "the same rights that people have offline must also be protected online".[36]

The UN followed this resolution with a series of activities. The Office of the High Commissioner for Human Rights (OHCHR) submitted a series of thematic reports to the UN Human Rights Council (UNHRC) and the UNGA, conducting a comprehensive and critical analysis of states' national legislations and enforcement mechanisms protecting the right to privacy.[37] The UNHRC also appointed a Special Rapporteur on the right to privacy and adopted several resolutions[38] highlighting the changing nature of threats to the right to privacy and recalling states' positive obligations to ensure that any interference with the right to privacy should be consistent with the principles of legality, necessity, and proportionality.[39] These recommendations are of utmost importance due to the partial inadequacy of international human rights treaties – adopted well before the Internet era – to address and solve the challenges posed to the right to privacy by the development of global surveillance technologies. Thus, the radical reinterpretation process of the existing scope of the right to privacy, and general adaptations with regard to the

34 UNGA 'The Right to Privacy in the Digital Age', UN Doc A/C.3/68/L.45 (November 2013).

35 Colum Lynch, 'Exclusive: Inside America's Plan to Kill Online Privacy Rights Everywhere' (Foreign Policy, November 20, 2013) <https://foreignpolicy.com/2013/11/20/exclusive-inside-americas-plan-to-kill-online-privacy-rights-everywhere/>.

36 UNGA Resolution 'The Right to Privacy in the Digital Age', A/Res/68/167 (December 2013); Since then, four additional UN GA Resolutions were adopted: Resolution 69/166 (December 2014), Resolution 71/199 (December 2016), Resolution 73/179 (December 2018, Resolution 75/176 (December 2020).

37 A/HRC/27/37 'The right to privacy in the digital age (Focus on surveillance)' (2014); A/HRC/39/29/ 'The right to privacy in the digital age' (2018); A/HRC/44/24 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests' (2020); A/HRC/48/31 'The right to privacy in the digital age (focus on artificial intelligence)' (2021).

38 HRC Resolution 28/16; HRC Resolution 34/7; HRC Resolution 32/2; HRC Resolution 42/15.

39 HRC Resolution 42/15.

interpretation and scope of application of existing norms, allow them to meet the new conditions of the digital age. As Yuval Shany notes with regard to the right to privacy, its continued relevance in the digital age was helped by the theoretical shift from a dominant conception of privacy as a right to be left alone to notions of privacy involving the right to exercise control over personal data and its derivative uses, including control over inter-personal communication flows.[40]

In 2018, the OHCHR proposed a UN Draft Legal Instrument on Government-Led Surveillance and Privacy, tackling the issue of domestic and foreign state surveillance "from a perspective which has international human rights protection and human dignity at its centre".[41] The Draft Legal Instrument attempted to limit surveillance activities by adopting a "reasonable suspicion" threshold, i.e., requiring a state to "demonstrate that the specific anticipated surveillance would yield evidence of a serious crime or help mitigate the threat".[42] It was, however, faced with pushback from states as varied as Brazil, Germany, China, and the US.[43] This pushback highlights that walking the human rights path to secure political support for subjecting states' intelligence activities to a set of international legally binding norms is tremendously challenging.

Virtually no space was left for the human rights agenda and the right to privacy in the GGE and OEWG reports. The 2015 GGE consensus report contained one important (non-binding) recommendation that states, in ensuring the secure use of ICT, should respect human rights and guarantee their full protection, including the right to privacy and freedom of expression.[44] Despite the vast consulting work of numerous NGOs on various facets of human rights, the 2021 report of the OEWG[45] does not mention the right to privacy at all.

The pushback on the right to privacy is part of a broader trend challenging the universalism of human rights. The rise of civilizational, cultural, and ideological confrontations in the human rights agenda is reflected in recent proposals of

40 Yuval Shany, 'Digital Rights and the Outer Limits of International Human Rights Law' (2022). 24 German Law Journal 465.

41 Office of the High Commissioner for Human Rights, UN Special Rapporteur on the Right to Privacy, 'Draft Legal Instrument on Government-led Surveillance and Privacy' (10 January 2018).

42 Ibid 10-11.

43 See, e.g., Stefan Talmon, 'No need for Legal Instrument on Electronic Surveillance and Privacy' (*German Practice in International Law*, June 5, 2018). < https://gpil.jura.uni-bonn.de/2018/06/no-need-legal-instrument-electronic-surveillance-privacy/ > accessed 27 November 2022; Monika Ermert, 'UN Rapporteur for Privacy Rebuffed on Surveillance Oversight Negotiations" (*Intellectual Property Watch,* March 7, 2018) < https://www.ip-watch.org/category/venues/regional-policy/page/26/ > accessed 27 November 2022.

44 UN GA Resolution (2015) UN Doc A/RES/70/174, Recommendation 13(e).

45 UN GA Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive report. (2021) UN Doc A/AC.290/2021/CRP.2.

the Codes of Conduct for Information Security 2012[46] and 2015,[47] which were sponsored by Russia and China and supported by the Shanghai Cooperation Organization (SCO). These two instruments, focusing primarily on peace and security issues, are unconditionally state-centric and raise substantial concerns with respect to human rights.[48] After a heavy critique of the first draft, the 2015 Code of Conduct repeated the widely used formula that human rights apply online as they do offline, yet without unpacking what this means in practice. The Code of Conduct also mentioned Article 19 of the ICCPR on freedom of expression but omitted any reference to the right to privacy. Such limited framework follows the aspiration of SCO member states to frame existing domestic information controls as compatible with international human rights.

Today, tensions over human rights in the cyber domain continue in the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes.[49] The Ad Hoc Committee held its first discussions in early 2022, resulting in a consolidated negotiating document prepared by the Chair in November 2022. The document stipulates the applicability of international human rights law in its general provisions (Article 5) and mentions briefly the protection of privacy in Article 42(1), which covers the "conditions and safeguards" for the exercise of the state powers in the fight against cybercrime.[50] During the first negotiations on this draft in January 2023, however, several states proposed to remove Article 42(1) fully or partially, claiming that the general reference to human rights in Article 5 already covers the protection of privacy.[51].

These repeated experiences confirm that, despite the technical universalism of ICT, there remains a strong pushback against the conceptual universalism of human rights in cyberspace. The momentum of internet sovereignty and the growing desire of states to control information means that soft law documents on a multilateral level remain the only possible way to advance the right to privacy

46 UNGA, 'Letter Dated 12 September 2011 for the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General' (12 September 2011) UN Doc A/66/359.

47 UNGA, 'Letter Dated 9 January 2015 for the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General' (9 January 2015) UN Doc A/69/723.

48 Watt (n 2) 97.

49 Deborah Brown, Opening Stages in UN Cybercrime Treaty Talks Reflect Human Rights Risks (Human Rights Watch, 28 April, 2022) <https://www.hrw.org/news/2022/04/28/opening-stages-un-cybercrime-treaty-talks-reflect-human-rights-risks> accessed 25 November 2022.

50 UNGA, 'Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes' (7 November 2022) UN Doc A/AC.291/16.

51 Karine Bannelier, The U.N. Cybercrime Convention Should Not Become a Tool for Political Control or the Watering Down of Human Rights (Lawfare, 31 January 2023) <https://www.lawfareblog.com/un-cybercrime-convention-should-not-become-tool-political-control-or-watering-down-human-rights> accessed 2 February 2023.

agenda in law-making efforts. To protect human rights, including the right to privacy against cyberespionage, an alternative solution is the use of the existing human rights framework and institutions. The next section assesses the difficulties, potential, and results of this path.

7.3 Curtailing cyberespionage through international human rights law

In the context of cyberespionage, individuals' cybersecurity is constantly jeopardized by states' and private companies' bulk collection and retention of personal data. In the absence of a multilateral treaty directly regulating states' cyber surveillance activities, international human rights law (IHRL) has been a natural medium to vindicate individuals' rights against increasingly expansive and intrusive practices of cyber surveillance. Yet, extending the scope of application of mid-20th century treaties to modern practices of global cyberespionage triggers many procedural issues, notably of standing and extraterritorial jurisdiction (7.3.1). In addition, it is anything but clear what the role of human rights should be in the balance of interests at stake. As a result, human rights courts confronted with the issue have evolved towards a case law that can be deemed less than satisfactory in curtailing cyberespionage (7.3.2).

7.3.1. Harnessing human rights against cyberespionage: Procedural issues

Cyberespionage triggers serious intrusions on human rights. Cyber surveillance, whether it is targeted or bulk (mass surveillance), infringes on individuals' right to privacy, but also many other human rights. Indeed, surveillance measures have a deep chilling effect on freedom of expression, religion, and movement, and can result in intrusions on the right to liberty of the person and the right to a fair trial, when data obtained through surveillance is used in administrative or judicial proceedings.[52] In consequence, IHRL has been a natural recourse to attempt to curtail the ever-expanding reach of cyberespionage on individuals' rights.

However, IHRL does not naturally fit well with modern practices of (foreign) (mass) cyber surveillance. Two admissibility matters, in particular, have been at issue, namely standing and jurisdiction. For IHRL to apply to cyberespionage, claimants need to show they are a victim *and* that the state spying on them owes them human rights obligations. Due to the nature of cyberespionage, these matters have necessitated judicial creativity, triggering procedural developments in IHRL.

With regard to standing, the issue is somewhat obvious. Surveillance being a secret activity, it is often impossible for an individual to prove that they are subject to it and thus that they are a victim deserving of standing before a court.[53]

52 Martin Scheinin, 'Impact of Post-9/11 Counter-Terrorism Measures on All Human Rights' in Manfred Nowak and Anne Charbord (eds), *Using Human Rights to Counter Terrorism* (Edward Elgar Publishing 2018).

53 See e.g., ECHR, Articles 34 and 35; ICCPR, First Optional Protocol, Article 2.

This issue is made even more salient in the cyber context as obtaining tangible proof of having been put under surveillance is no longer a possibility, except in singular cases.[54] The only court confronted with this matter, however, has adapted to this factual situation – potentially leading the way for other courts and bodies. In the 2015 case of *Roman Zakharov* v. *Russia*, the European Court of Human Rights (ECtHR) allowed individuals to claim victim status on the ground that the existence of secret surveillance methods, or legislation permitting their use, could be sufficient to show that there exists a risk of being subjected to them.[55] With victim status granted to potentially all victims of secret surveillance measures, the matter can be brought before the ECtHR for a human rights appraisal provided the other main admissibility condition – jurisdiction – is satisfied.

Human rights jurisdiction is grounding: it constitutes the necessary relationship between the state and the individual, giving rise to rights and obligations.[56] Establishing jurisdiction is a straightforward endeavor when a violation happens on the state's territory.[57] However, existing surveillance programs in cyberspace know virtually no borders. Hence, anyone anywhere in the world could potentially be subjected to secret surveillance by any state having the technical means to do so. Can anyone bring a claim against any state?

Human rights courts and bodies have developed two main models to extend states' obligations beyond their territory. Accordingly, extraterritorial jurisdiction arises either when the state exercises de facto effective control over part of a territory abroad (spatial model)[58] or when the state exercises authority and control over an individual (personal model).[59] The UN Human Rights Committee (CCPR) has gone further in both its case law and in General Comment No. 36 by affirming that extraterritorial jurisdiction can also arise when the state holds "control over rights". In other words, the state exercises jurisdiction over "all persons over

54 In the context of targeted cyberespionage through Pegasus spyware, it has become possible to test whether one's phone has been penetrated.

55 *Roman Zakharov* v. *Russia*, App. No. 47143/06, 4 December 2015, para 167.

56 Lea Raible, *Human Rights Unbound: A Theory of Extraterritoriality* (Oxford University Press 2020).

57 See, e.g., ECHR Article 1; ICCPR Article 2(1); ACHR Article 1(1). The ACHPR does not have a provision concerning jurisdiction.

58 International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion* [2004] ICJ Reports 2004 136, paras 109-11; *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, ICJ Reports 2005*, 168, paras 179 and 216-217; ECtHR *Loizidou* v. *Turkey* (preliminary objections), App. No. 15318/89, 23 February 1995, para 62; UNCAT, 'Conclusions and recommendations: United Kingdom of Great Britain and Northern Ireland', UN Doc. CAT/C/CR/33/3, 10 December 2004, para 4(b).

59 ECtHR, *Cyprus* v. *Turkey*, App. Nos. 6780/74 and 6950/75, 26 May 1975, para 8; *Al-Skeini and Others* v. *The United Kingdom*, App. No. 55721/07, 7 July 2011, para 136; CCPR, *Lopez-Burgos* v. *Uruguay*, CCPR/C/13/D52/1979, 29 July 1981, paras 12.2-12.3; UNCAT, 'Consideration of Reports Submitted by States Parties under Article 19 of the Convention, United States of America', UN Doc. CAT/C/ USA/CO/2, 25 July 2006, para 20.

whose enjoyment of the right to life it exercises power or effective control"[60] or "if it is a link in the causal chain that would make possible violations in another jurisdiction".[61] The Inter-American Court of Human Rights (IACtHR), in its first confrontation with the question of extraterritorial jurisdiction, also recognized the "control over rights" approach as a third model of extraterritorial jurisdiction.[62]

When it comes to extraterritorial jurisdiction in matters of cyberespionage, we need to distinguish two factual situations linked to victim status and attribution. In the first, an individual asserts that they may be subjected to cyber surveillance, for instance, on the basis that the state has passed legislation authorizing indiscriminate mass surveillance; in the second, the individual knows they have been subjected to cyber surveillance, for instance, because their phone has been confirmed to be infiltrated by Pegasus spyware.[63]

The first situation relies on the existence of practice or legislation permitting cyber surveillance, as in *Zakharov*, and attribution to the state is not at issue. The only matter to be assessed is whether the individual is within the state's jurisdiction, as defined by the relevant interpreter of the treaty. If the individual is within the state's territory, then jurisdiction is automatically established. In contrast, if the individual is outside the state's territory and extraterritorial jurisdiction is contested by the respondent state,[64] then extraterritorial jurisdiction will need to be found under one of the models developed by courts and bodies. It bears mentioning that the spatial and personal models do not quite fit extraterritorial cyber surveillance, and existing case law does not help to clarify whether and how they could apply to such situations.[65] In contrast, the "control over rights" model, because it finds extraterritorial jurisdiction provided a causal link between the state's acts and the wrong suffered by the complainant can be established, could more easily cover cyberespionage. The issue, however, would be that of proving such a causal link where cyber surveillance is, by nature, a secret activity and the individual might not even know whether their personal data has been collected. Whether the chilling

60 UN CCPR, 'General Comment No. 36, Article 6 (Right to Life)' (2019) CCPR/C/GC/36 para 63.

61 *Munaf* v. *Romania*, CCPR/C/96/D/1539/2006, 21 August 2009, para 14.2.

62 *Advisory Opinion OC-23/17 of November 15, 2017 Requested by the Republic of Colombia: The Environment and Human Rights*, Inter-American Court of Human Rights (IACtHR), para 104(h): 'When transboundary harm or damage occurs, a person is under the jurisdiction of the State of origin if there is a causal link between the action that occurred within its territory and the negative impact on the human rights of persons outside its territory. The exercise of jurisdiction arises when the State of origin exercises effective control over the activities that caused the damage and the consequent human rights violation.'

63 David Pegg and Sam Cutler, 'What Is Pegasus Spyware and How Does It Hack Phones?' *The Guardian* (18 July 2021) <https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones> accessed 15 March 2022.

64 This is not always the case. For instance, in *Big Brother Watch* (n 21), the UK did not contest that it had jurisdiction over claimants located in Ireland, and the ECtHR abstained from addressing this issue.

65 For further analysis of extraterritorial jurisdiction in cases of foreign surveillance, see Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard International Law Journal 66.

effect of being a potential victim of foreign cyber surveillance will be enough to constitute a wrong establishing both standing and extraterritorial jurisdiction before the CCPR or the IACtHR remains an open matter.

In the second situation, attribution is a prerequisite and might even constitute a sufficient condition for jurisdiction, depending on the extraterritorial jurisdiction model adopted. In this situation, the CCPR's and IACtHR's "control over rights" model would be particularly appropriate for cases where attribution can be established. Should the claimant be unable to prove attribution, however, establishing jurisdiction would require courts to shift the burden of proof onto the respondent state. This has been done by the ECtHR in CIA-related cases,[66] and one could presume that the underlying justification (namely that the respondent state is the only entity with exclusive knowledge of the facts) could also apply to cases of surveillance.

The issue of extraterritorial jurisdiction might lead us to question the very relevance of IHRL in regulating cyberespionage happening on a global scale. As Yuval Shany summarizes it, "the fit between a territory-driven state-centric legal framework based on physical presence and the actual dynamics of virtual social interactions [in] cyberspace is very limited".[67] Human rights courts, and particularly the ECtHR and the CJEU, have nevertheless managed to substantively address the human rights implications of cyberespionage.

7.3.2. Cyberespionage in human rights practice: A matter of substantive balancing?

Cyber surveillance infringes particularly on individuals' right to privacy. This right being non-absolute, it can be restricted. Human rights courts and bodies then have the task of assessing whether the interference with the right: 1) is in accordance with law; 2) serves a legitimate aim;[68]and 3) is proportionate to the aim pursued.[69] The balance between the right to privacy and the competing legitimate aim justifying its restriction has been struck differently by various courts and bodies, and it is still an evolving one. In Europe, where the only supra-national case law on

66 ECtHR, *El-Masri* v. *The Former Yugoslav Republic of Macedonia*, Judgment, 13 December 2012, App. No. 39639/09*,* paras 151-153; *Al-Nashiri* v. *Poland*, Judgment, 24 July 2014, App. No. 28761/11, paras 395-396; *Husayn (Abu Zubaydah)* v. *Poland,* Judgment, 24 July 2014, App. No. 7511/13, paras 395-396.

67 Yuval Shany, 'Cyberspace: The Final Frontier of Extra-Territoriality in Human Rights Law' (2017): https://csrcl.huji.ac.il/people/cyberspace-final-frontier-extra-territoriality-human-rights-law.

68 See, e.g., the list of legitimate aims provided in Article 8(2) ECHR: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

69 ECHR, Article 8; CCPR, General Comment No. 16: Article 17 (Right to Privacy) (1994) CCPR/C/GC/16; Donoso v. Panama (Judgment), IACtHR, para 56 (Jan. 27, 2009).

mass surveillance and indiscriminate data retention is to be found, a trend towards proceduralism and an increased legitimation of these practices is emerging.

As explained in the Introduction, justifications for surveillance practices usually present a phenomenon such as terrorism as a threat to a legitimate interest, such as national security or public order. To prevent the threat from materializing, states argue that surveillance is not only needed, but also lawful under IHRL. The justification constructs the threat as triggering a legitimate exception to the rule (the right to privacy) and presents the response (surveillance) not as a violation of the rule but as a necessary and proportionate interference with it. The result is that governments often present bulk data collection and retention or spyware like Pegasus as lawful.[70] Only if (international) courts get involved can the rhetorical use of IHRL forming the justification be legally evaluated and deconstructed.

Despite starting as rather protective of human rights in their initial assessments of surveillance and data retention practices, European courts have gradually moved towards a balance more deferential to states' national security assessments and claimed needs for mass surveillance. In so doing, the ECtHR and CJEU have gradually legitimized mass surveillance and indiscriminate data retention.

Starting in the aftermath of 9/11, the ECtHR endorsed in principle the strategic surveillance of foreign communications as falling within states' wide margin of appreciation[71] in *Weber and Saravia* v. *Germany*[72] and *Liberty and Others* v. *UK*.[73] With its 2021 Grand Chamber judgments in *Big Brother Watch* (BBW) and *Centrum för Rättvisa* (CFR),[74] the Court extended this endorsement to mass surveillance by considering that operating a bulk interception regime is not, in principle, unlawful and/or disproportionate. The Court thus found that the British and Swedish bulk interception regimes under consideration were "valuable"[75] and of "vital importance"[76] to the security of member states – notwithstanding the lack of evidence concerning their actual performance. On this basis, the Court confirmed that national authorities enjoy a "wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security".[77] Through these two judgments, the Grand Chamber thus affirmed the legitimacy of mass surveillance,

70 Note that the 'in accordance with law' prong of the proportionality assessment is almost always left out of such justifications.

71 Eliza Watt, 'Much Ado About Mass Surveillance – the ECtHR Grand Chamber "Opens the Gates of an Electronic 'Big Brother' in Europe" in Big Brother Watch v UK' (*Strasbourg Observers*, 28 June 2021) <https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/> accessed 30 June 2021.

72 Application No. 54934/00, 29 June 2006.

73 Application No. 58243, 1 July 2008.

74 *Big Brother Watch and Others* v. *The United Kingdom* [GC], Applications Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021; *Centrum för Rättvisa* v. *Sweden* [GC], Application No 35252/08, 25 May 2021.

75 BBW para 323, CFR para 237.

76 BBW para 424, CFR para 365.

77 BBW para 228, CFR para 252.

succumbing to what Monika Zalnieriute called the "inevitability of securitisation narrative".[78]

The consequence of this finding, for the majority of the Grand Chamber, is that end-to-end safeguards are needed. The Court thus establishes a new eight-part test to assess the compatibility of bulk regimes with Article 8 ECHR.[79] The test, as applied in both cases, focuses on the regulatory framework and procedural safeguards rather than on actual practice. In other words, the test assesses exclusively the "in accordance with law" prong of the broader proportionality assessment and assumes satisfaction of the "legitimate aim" and "proportionality" prongs. Indeed, both decisions exemplify the Court's blind trust in the state's assessment that interception, storage, and analysis of data and metadata are necessary and proportionate to protect national security.[80] As Marko Milanovic concludes, the two judgments constitute a definitive normalization of mass surveillance.[81]

The proceduralist approach[82] to mass surveillance adopted by the ECtHR greatly facilitates states' legitimation of their bulk collection regimes. Provided states' regulatory frameworks respect the eight-part (procedural) test established by the Grand Chamber, the regime will be deemed in accordance with law. States can then legitimate any bulk regime satisfying this test by presenting the regime as necessary and proportionate – and thus lawful. Based on the two decisions, it seems that whether this regime is actually "valuable" and whether the practice complies with the regulatory framework are of virtually no importance for the outcome

78 Monika Zalnieriute, 'Big Brother Watch and Others v. the United Kingdom' (2022) 116 American Journal of International Law 585.

79 BBW para 361, CFR para 275. The test purports to assess jointly the 'in accordance with law' and 'necessity' aspects of the surveillance regime by examining 'whether the domestic legal framework clearly defined:the grounds on which bulk interception may be authorised;

1. the circumstances in which an individual's communications may be intercepted;
2. the procedure to be followed for granting authorisation;
3. the procedures to be followed for selecting, examining and using intercept material;
4. the precautions to be taken when communicating the material to other parties;
5. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
6. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
7. the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.'

80 Massimo Frigo, 'Big Brother Watch v. UK: A Landmark Judgment Missing the Mark' (*Opinio Juris*, 4 June 2021) <http://opiniojuris.org/2021/06/04/big-brother-watch-v-uk-a-landmark-judgment-missing-the-mark/> accessed 7 June 2021.

81 Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum För Rättvisa' (*EJIL: Talk!*, 26 May 2021) <https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/> accessed 16 March 2022.

82 Monika Zalnieriute, 'Procedural Fetishism and Mass Surveillance under the ECHR' (*Verfassungsblog*) <https://verfassungsblog.de/big-b-v-uk/> accessed 16 March 2022.

of a case. In a more recent case concerning domestic surveillance, the Court nevertheless underlined that procedural safeguards should not only exist on paper but also operate in practice.[83] Despite this welcome if belated reminder regarding the "in accordance with law" prong of the proportionality test, the ECtHR's case law still provides states with considerable political and legal legitimation for their mass surveillance programs.

In contrast, the Court of Justice of the European Union (CJEU) was originally more protective of privacy rights in its case law on mass surveillance and data retention. Its initial pronouncement in *Digital Rights Ireland*[84] annulled the Data Retention Directive[85] and rejected a model of mass surveillance based on general and indiscriminate retention of communication metadata as incompatible with the Charter of Fundamental Rights of the European Union (CFREU).[86] In this landmark judgment, the CJEU thus rejected the possibility that indiscriminate data retention could be a proportionate interference with the right to respect for private and family life (Article 7 CFREU) and to the protection of personal data (Article 8 CFREU). The Court's principled opposition to mass surveillance was reaffirmed in further cases concerning national data retention regimes in EU Member States;[87] international data sharing;[88] and the transfer of Passenger Name Record (PNR) data.[89]

However, in its 2020 decisions in *Privacy International*[90] and *La Quadrature du Net and Others*,[91] the CJEU reversed its previous principled stance by introducing a national security exception. While *Privacy International* reaffirmed the incompatibility with EU law of mass transmission of personal data by commercial operators to intelligence agencies, *La Quadrature du Net,* delivered on the same day, authorized indiscriminate data retention measures on national security grounds. Signaling a newfound convergence with the ECtHR, *La Quadrature*

83 *Ekimdzhiev and others* v. *Bulgaria*, Application No. 70078/12, 11 February 2022, para 419.

84 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others (C-293/12) and Kärntner Landesregierung and Others (C-594/12) [2014] ECLI:EU:C:2014:238.

85 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services of public communications networks and amending Directive 2002/58/EC,OJ L105/54, 13.4.2006 (Data Retention Directive).

86 Charter of Fundamental Rights of the European Union (2007/C 303/01).

87 Joined Cases C-203/15 and C-689/15, Tele2 Sverige AB v. Postoch telestyrelsen (C-203/15) and Secretary of State for the Home Department v. Tom Watson and Others (C-689/15) [2016] ECLI:EU:C:2016:970.

88 C-362/14 Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650 and C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559.

89 Case Opinion 1/15, ECLI:EU:C:2016:656.

90 Case C-623/17, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others, ECLI:EU:C:2020:790.

91 Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v. Premier Ministre and Others, ECLI:EU:C:2020:791.

du Net results in the principled acceptance of mass data retention (and thus mass surveillance as a necessary prior step) as a proportionate interference with human rights when the legitimate aim pursued is the protection of national security. The national security exception was reaffirmed in a later decision, a preliminary ruling concerning Germany's telecommunications data retention law, although in this case the legislation at stake was judged non-compliant with EU law.[92] As the ECtHR did in *Big Brother Watch* and *Centrum för Rättvisa*, the CJEU attempts to limit the mass data retention under the national security exception by mandating procedural safeguards. Yet, the CJEU's convergence with the ECtHR's principled acceptance of mass surveillance as inevitable and necessary has serious consequences for any hope of curtailing the practice and its development.

This legitimizing trend has been confirmed by another CJEU decision concerning mass surveillance and indiscriminate data retention. In *Ligue des Droits Humains*,[93] concerning the Passenger Name Record (PNR) Directive,[94] the Court approved the surveillance regime established by the PNR Directive as compatible with the CFREU. In so doing, the Court took a different path than it had done in *Digital Rights Ireland,* where it annulled the Data Retention Directive on the ground that indiscriminate data retention would be incompatible with fundamental rights. In *Ligue des Droits Humains*, instead, the CJEU strictly circumscribed the PNR Directive's transposition into Member States' national law through a restrictive interpretation of its provisions (leading to its alteration "beyond recognition"[95]). The difference between its landmark 2014 case and this 2022 ruling lies in the acceptance of mass surveillance as a proportionate and legitimate measure to face national security threats. The European normalization of mass surveillance is thus complete, leaving few hopes of meaningfully constraining and curtailing the development of mass surveillance through human rights courts in the region.

7.4 Conclusions

With states unable to agree on an international legal framework to govern cyberespionage, human rights courts have a crucial role to play in curtailing the expansion of intrusive surveillance methods and indiscriminate data retention. Following the Snowden revelations, European courts have been tasked with assessing whether states' mass surveillance programs were compatible with regional human rights frameworks. They thus had a valuable opportunity to draw

92 Joined Cases C-793/19 (SpaceNet AG) and C-794/19 (Telekom Deutschland), ECLI:EU:C:2022:702.

93 Case C-817/19, Ligue des Droits Humains v. Council of Ministers, ECLI:EU:C:2022:491. For a commentary, see Sophie Duroy, 'Case C-817/19, Ligue Des Droits Humains v. Council of Ministers (C.J.E.U.)' (2023) 62 International Legal Materials 611.

94 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

95 Christian Thoennes, 'A Directive altered beyond recognition' (*Verfassungsblog*, 23 June 2022) <https://verfassungsblog.de/pnr-recognition/> accessed 8 November 2022.

some clear lines and curtail the ever-expanding reach of cyberespionage over human rights. However, the balance struck in Europe disproportionately favors states' national security policies and legitimizes mass surveillance and indiscriminate data retention.

Rather than remedying the lack of multilateral norms governing cyberespionage, the case law developed by European courts might further negatively influence law-making efforts on the international stage. Indeed, the legitimation of mass surveillance granted by European courts has the potential to carry over to law-making at both European and international levels.[96] In the EU, future Directives and Regulations will necessarily take into account the CJEU's latest case law to ensure conformity with the CFREU. In particular, the Council of the European Union has proposed that the new ePrivacy Regulation,[97] currently being developed to replace the ePrivacy Directive,[98] should clearly exclude national security activities from its scope.[99] Such a development would imply that the (bulk) collection and retention of private data for national security purposes would not fall under the scope of the Regulation, thus leaving states and private providers unconstrained by its provisions. In multilateral forums, European courts' principled acceptance of mass surveillance and indiscriminate data retention might further hinder efforts to bring human rights to the forefront of discussions.

As a result, the protection of the right to privacy in cyberspace, and more generally of human rights in the digital age, appears highly compromised. Furthermore, with states unable to agree on an international legal framework, remaining opportunities to curtail cyberespionage are few. Two such opportunities might come to mind, namely domestic courts and human rights courts and bodies beyond Europe. As for domestic courts, the German Constitutional Court issued a very progressive ruling in 2020, holding that German intelligence services are bound by human rights law in all their activities, and even when acting abroad.[100] The Court's approach to extraterritoriality in this case was agency-focused. In other words, what mattered for the Court is that German intelligence services behave in accordance with human rights in all their activities, and not that anyone anywhere holds enforceable rights against the German state. By focusing on the

96 Zalnieriute (n 78) 591–592.

97 *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)* - COM/2017/010 final - 2017/03 (COD).

98 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

99 *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)—Mandate for negotiations with the European Parliament*, ST 6087 2021 INIT (10 February 2021).

100 Bundesverfassungsgericht [BVerfG – Federal Constitutional Court], May 19, 2020, Case No. 1 BvR 2835/17.

standard of behavior of state entities, this promising approach would be replicable by other domestic courts. Furthermore, these higher domestic standards can impact intelligence cooperation and sharing and might thus have an effect on other states through the "trickle down" effects[101] of the normative benchmarks constraining German intelligence services.[102]

Beyond Europe, the UN Human Rights Committee (CCPR) and the Inter-American Commission (IACHR) and Court (IACtHR) have yet to rule on the conformity of mass surveillance with the right to privacy under their respective human rights frameworks.[103] Given their usually progressive case law, and especially their broader conception of extraterritorial jurisdiction, a decision by the CCPR, the IACHR, or the IACtHR might provide more protection to individuals than in the European system. Should the CCPR rule on cyberespionage and adopt a broader understanding of extraterritoriality, this would also have an effect in Europe, thereby counteracting the permissive effects of existing case law in this respect. In this context, strategic litigation would thus be a valuable option towards achieving a better balance between the competing human rights in the liberty-security equation. As we have shown, while this equation can be presented as a struggle for global cybersecurity against the temptation of unlimited cyberespionage by states and private companies, it is at its core a balancing act between the protection of human rights and the legitimate aims justifying their restriction.

101 Ashley Deeks, 'Intelligence Services, Peer Constraints, and the Law' in Zachary K Goldman, Samuel J Rascoff and Jane Harman (eds), *Global Intelligence Oversight* (Oxford University Press 2016).

102 On this aspect, see Katrin Kappler, 'Consequences of the German Constitutional Court's Ruling on Germany's Foreign Intelligence Service: The Importance of Human Rights in the Cooperation of Intelligence Services' (2022) 23 German Law Journal 173.

103 There is no right to privacy in the African Charter on Human and Peoples' Rights.