Introduction

This chapter examines the extent to and the basis on which human rights treaties apply extraterritorially to state surveillance and cyber operations. Consider only the following examples:

1. The targeted surveillance of a specific individual outside a state’s territory – as, for instance, with the operations allegedly conducted by the authorities of Saudi Arabia against Saudi dissidents abroad (see, e.g., Kirchgaessner and Hopkins 2019; Kirchgaessner 2020) (one of which ultimately led to the plot to assassinate the journalist Jamal Khashoggi (see, e.g., Kirkpatrick 2018; for more on the Khashoggi affair, see Callamard 2020; Milanovic 2020), or against the CEO of Amazon, Jeff Bezos, apparently in a rather crude attempt to blackmail him (see Office of the United Nations High Commissioner for Human Rights (OHCHR) 2020).

2. Mass surveillance or bulk collection programmes, such as those run by the US and UK signals intelligence agencies, that syphon the content of electronic communications of millions of people outside the state’s territory, or the metadata about these communications, in order to create searchable datasets in which persons of particular interest, e.g. suspected terrorists, can then be found (see Macaskill and Dance 2013).

3. Cyber operations that exfiltrate data on COVID-19 vaccine research, potentially affecting the development of vaccines that could save many thousands of lives (see Akande et al. 2020a).

4. Cyber operations that destroy or manipulate such data.

5. Cyber operations against hospitals or against critical infrastructure, which directly endanger many lives (see Akande et al. 2020b).

6. Cyber operations against media outlets, which disrupt their activities and inhibit their freedom of expression.

7. Online misinformation operations for various purposes, for example, to manipulate the outcome of an election or to destroy public trust in state institutions during the pandemic (see more Milanovic and Schmitt 2020).
The list above is obviously not meant to be exhaustive. What all of these examples have in common, however, is that through entirely digital means states can violate a host of different human rights, from the rights to privacy and the freedom of expression, to the right to life and the right to health, of persons located outside their territories.

The question of the extraterritorial application of human rights treaties has long been a vexing one. It has been especially contentious in situations of armed conflict, for instance, with regard to detention and use of force operations. In my prior work, I have advocated for an expansive and factual approach to the extraterritorial application of human rights treaties, arguing in particular that the negative obligation to respect human rights should be territorially unrestricted (see Milanovic 2011, p. 209 et seq.). With regard to extraterritorial surveillance in particular, I have similarly argued that any state surveillance operation that interferes with the privacy of individuals abroad would engage the relevant treaties and would require justification within the human rights framework (see Milanovic 2015).

In this chapter, I will address the extraterritorial applicability both of ‘pure’ surveillance operations, which only involve the exfiltration of personal data through digital or analogue means, and other kinds of cyber operations, which may affect numerous human rights and not just privacy. The key point in that regard is that if surveillance operations are covered then, a fortiori, so are other cyber operations that can have substantially more severe impacts on individuals than the mere exfiltration of data.

The chapter will first proceed to briefly outline how the traditional models of extraterritorial application, the spatial and the personal, would apply to surveillance and cyber operations, examining a few old cases in which the issue was raised, if never properly resolved. It will then look at recent developments that are particularly important in the surveillance and cyber context, even if some of them are not directly apposite: a judgment of the UK Investigatory Powers Tribunal, the advisory opinion of the Inter-American Court of Human Rights on the environment and human rights, the Human Rights Committee’s General Comment no. 36 on the right to life and the judgment of the Federal Constitutional Court of Germany on the applicability of the German Basic Law to surveillance operations abroad. The chapter will then finally offer some concluding thoughts on the direction towards which the legal position is likely to evolve, and should evolve, regarding the applicability of human rights law to extraterritorial surveillance and cyber operations.

**Surveillance and cyber operations under the traditional models of extraterritorial application**

Many human rights treaties, among them the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights (ECHR) and the American Convention on Human Rights (ACHR), use the notion of state jurisdiction to delineate their scope of application. Human rights courts and treaty bodies have interpreted that notion in two basic ways – as state control over a territory in which the victim of the human rights violation is located (the spatial conception or model of jurisdiction), or as state authority, power or control over the victim directly, exercised by one of the state’s agents (the personal conception or model of jurisdiction) (see more Milanovic 2011, pp. 127–208). Yet, some treaties, like the International Covenant on Economic, Social and Cultural Rights (ICESCR), contain no jurisdiction clauses, and it is even less clear how customary human rights law applies extraterritorially, although arguments have been made in favour of the unrestricted application of negative customary obligations (see, e.g., Heyns et al. 2016, p. 823).

How would the two traditional extraterritoriality models apply to surveillance and cyber operations? With one caveat, the application of the spatial model would be reasonably
straightforward. If an individual was located in a territory under the effective overall control of a state, even if that territory was not under the sovereignty of that state, the individual concerned would enjoy full protection for their privacy and any other relevant human rights vis-à-vis that state. For example, if a person in Crimea was subjected to electronic surveillance by the authorities of the Russian Federation, the ECHR would apply to that surveillance regardless of the fact that Russia does not possess title to Crimea, an area which nominally remains under Ukrainian sovereignty under international law. If a case presenting such facts were to come to the European Court, it would not need to resolve the disputed question of sovereignty over the territory. All the Court would need to establish was that, as a matter of fact, Russia exercises effective control of the area, regardless of whether that control was obtained lawfully or unlawfully (see, e.g., European Court of Human Rights (ECtHR) 1995, para. 62; see more Milanovic 2015, pp. 122–124).

The spatial applicability of human rights treaties in such circumstances to me seems uncontestable. But now for the caveat: it is also possible that human rights bodies would apply the spatial model to scenarios in which the surveillance or cyber operations targets the data of an individual that physically transits or is located in a state’s territory, even while the individual themselves is located outside it. Consider the following example: while I am writing this, I am physically located in Belgrade, the capital of Serbia. But were British authorities to conduct a search of my flat in Nottingham, and seize documents or data that they find there even while I am myself out of the country, there would be no doubt whatsoever that the ICCPR and the ECHR would apply to such a search. The more contested issue, which I will turn to in a moment, is the precise conceptual basis of the treaties’ applicability, which must be extraterritorial since I, as the bearer of the relevant rights, am outside the state’s territory even while the state is interfering with these rights solely by acting on its own territory.

A cyber analogy is reasonably direct. Were the UK to, say, intercept my emails or take control of data located on its own territory, for instance, by syphoning the data from an undersea cable that transits its territory or by seizing it from a UK-based cloud server, the position should be no different than in the example of the physical search of my apartment above. I, at least, see no plausible way of distinguishing the two; if the first is covered, on whatever basis, then so must be the second (see Milanovic 2015, pp. 124–127; Nyst 2013).

This brings us to the applicability of the personal model, that of authority, control, power over the victim exercised by state agents. This is a significantly more complex issue, both generally and with regard to surveillance and cyber operations specifically. In particular, the jurisprudence of the European Court has simultaneously been the most varied and the most restrictive in this regard. It is uncontested that detaining a person, i.e. state agents having physical custody over an individual, is an exercise of authority, control or power of them sufficient to create a jurisdictional link between the state and the victim (ECtHR 2014, paras. 74–80). It remains contested whether kinetic uses of lethal force against an individual without detaining them, for example, by firing a missile from a drone, constitutes authority or control over the person.

The most notorious and restrictive such case is of course Bankovic, in which the European Court held that an individual would not be within a state’s jurisdiction in the sense of Article 1 ECHR solely on the basis that the state dropped a bomb on them from the air, and did so partly on the erroneous basis that the concept of state jurisdiction in human rights treaties had something to do with the concepts of prescriptive and enforcement jurisdiction as aspects of state sovereignty (ECtHR 2001). Other cases followed, some of which implicitly partially overruled Bankovic, most notably Al-Skeini (ECtHR 2011), but the Court has nonetheless remained reluctant to extend the reach of the Convention to purely kinetic uses of force abroad, as it is morally and logically compelled to do (see generally Milanovic 2012, pp. 127–133). Despite the
Court's holding in *Al-Skeini* that the use of physical force against an individual by a state agent can constitute the exercise of authority or control over that individual, and thus state jurisdiction, and its holding that when a state exercises such authority and control over an individual it only needs to secure those rights of that individual that are relevant to his or her situation, so that rights under the ECHR can be divided and tailored (ECtHR 2011, paras. 136–137), the Court has still preserved the result and conceptual basis of *Bankovic*.

Following the logic of *Bankovic*, if dropping a bomb on someone would not suffice to create a jurisdictional link extraterritorially, then neither would be reading their emails nor the hacking of their phone. But that logic is misguided simply because *Bankovic* was wrongly decided. As I have argued before, the personal conception of jurisdiction as authority, power or control over individuals is prone to collapse to the proposition that negative obligations should apply without any territorial restriction; any purported limits appear to be arbitrary (see Milanovic 2011, pp. 207–208). As a thought experiment to test that argument, consider the following scenarios; suppose that all of them take place in Berlin and involve a hypothetical Angela Merkel:

1. A CIA agent grabs Angela Merkel, disables her escort (assume he is some kind of judo master) and then physically searches her for items in her possession.
2. A CIA agent breaks into and searches Angela's apartment and plants cameras and listening devices.
3. A CIA agent manages to get Angela's phone when she is not looking, and furtively plants a tracking device in it.
4. A CIA agent breaks into Angela's office and hacks into her computer, uploading a virus and downloading sensitive data.
5. A CIA agent observes and listens to Angela using a high-resolution camera/directed mike.
6. A CIA agent observes and monitors Angela's residence from the outside using a high-resolution camera/directed mike, without necessarily observing Angela herself.
7. A CIA agent hacks Angela's phone or computer remotely.
8. A CIA agent intercepts Angela's calls, texts or emails midstream.
9. A CIA agent is able to collect information about whom Angela calls, when, for how long (telephony metadata) or whom and when she mails (internet metadata).
10. The NSA obtains Angela's personal information from its partners in GCHQ, and stores and processes that information.

The scenarios progress from the more physical to the more virtual. There is, in my view, no point along this spectrum that could be picked as some non-arbitrary dividing line between the existence of jurisdiction and the lack thereof. If (1) is covered, then so is (2); if (2) is covered, then so is (3), etc. The personal model simply collapses, with the bottom line being that the state should comply with its negative obligation to respect human rights whenever it is able to do so (see Milanovic 2015, pp. 127–129). Any state surveillance activity abroad, and any cyber operation adversely affected human rights, would therefore be within the ambit of human rights treaties.

Human rights bodies are yet to grapple with this set of issues directly enough. I will canvass some relevant recent developments in that regard in a minute, but first let us briefly look at some of the relevant older, pre-Snowden jurisprudence.

In that regard, the only human rights body to have decided cases dealing with extraterritorial surveillance has been the European Court. Notably, at least two surveillance cases before the Court dealt with situations, we looked at above in which the interference was territorial while the individual was outside any area under the state's control. In the first, *Weber and Saravia v. Germany*...
(ECtHR 2006), the applicants lived in Uruguay while their communication was allegedly intercepted in Germany. Germany actually even objected (ibid, para. 66) that the case was outside its jurisdiction under Bankovic, but the Court avoided the matter (ibid, para. 72) and dismissed the case as manifestly ill-founded on other grounds. In the second, Liberty and Others v. the United Kingdom (ECtHR 2008), two of the applicants were Irish organisations that had communicated with the third, a British one, and their communication was allegedly intercepted in the UK by British authorities. Neither the UK government nor the Court proprio motu considered that an Article 1 jurisdiction issue arose with respect to the Irish applicants, i.e. they both assumed that the ECHR applied, and the Court went on to find a violation of Article 8 (see Milanovic 2015, p. 127).

For its part, the UN Human Rights Committee expressed concern about the mass surveillance programmes disclosed by Edward Snowden in its concluding observations regarding the US and the UK. The concluding observations simply assume the extraterritorial applicability of the ICCPR to these surveillance activities, but without articulating a clear basis for doing so. The Committee is yet to hear an individual case that deals with extraterritorial surveillance or other cyber operations.

Relevant recent developments

IPT judgment in Human Rights Watch and Others

The case most directly on point regarding the extraterritorial application of human rights treaties to surveillance actually comes from a domestic court – the UK Investigatory Powers Tribunal, in a case concerning the US and UK mass surveillance programmes (Investigatory Powers Tribunal 2016). Briefly, the Tribunal found the ECHR to be entirely inapplicable to extraterritorial surveillance, directly relying on a Bankovic analogy (ibid, paras. 56–61):

In so far as their claim is founded on belief that their right to respect for their private life has been infringed, neither of [the claimants] allege that, at any material time, they enjoyed a private life in the United Kingdom. Accordingly, under Article 1, the United Kingdom was under no obligation to respect it. The analogy with Bankovic is close. … Accordingly, the retention by GCHQ of information shared with it by the NSA, even in circumstances which do not comply with UK law, could not amount to a breach of the two Claimants’ right to respect for their private life.

(ibid, para. 58)

If Bankovic is correctly decided, at least for ECHR purposes, then the analogy would indeed be hard to resist – it would be absurd to accept that intercepting an individual’s email while they are abroad would constitute a jurisdictional link, whereas killing them with a bomb would not. It is thus unsurprising that the Tribunal ruled as it did, and that any corrections to Bankovic would have to happen in Strasbourg (cf. ibid, para. 60). The Tribunal also must be right that the applicability of the Convention cannot depend on whether the individual subjected to surveillance is located in the territory of some Convention state party other than the one doing the surveillance, rather than in a third state (ibid, para. 55 referring to the espace juridique concept). However, the Tribunal only superficially dealt with the import of the scenario in which interception happens territorially, even if the individual is located outside the state’s territory (ibid, para. 59; see more Kim 2016). As of the time of writing, the European Court is yet to address either this scenario or those of ‘pure’ extraterritorial surveillance, having managed to avoid the extraterritoriality issues in the cases it has examined so far, as I will explain below.
IACtHR Advisory Opinion on the Environment and Human Rights

A more promising development, but less directly apposite, is the 2017 advisory opinion of the Inter-American Court on the environment and human rights (IACtHR) (2017). The opinion has nothing to do with surveillance or cyber operations as such – indeed the Court and the Inter-American Commission are yet to hear any such cases. But the opinion provides us with the first genuinely systematic attempt by the Court to interpret the meaning of the term ‘jurisdiction’ in Article 1(1) ACHR and the scope of the Convention’s extraterritorial application (for detailed analysis, see Vega-Barbosa and Aboagye 2018; Feria-Tinta and Milnes 2018).

In that regard, the advisory opinion is something of a mixed bag. It sets out the travaux of the Convention (IACtHR 2017, paras. 71–78) and the relevant international jurisprudence (ibid, paras. 79–81), and (troublingly) endorses the Bankovic dictum of the European Court that extraterritorial jurisdiction is exceptional and that circumstances giving rise to such jurisdiction should be interpreted restrictively (ibid, paras. 81 and 104). Even worse, it endorses the Bankovic conceptual confusion between the notion of jurisdiction in human rights treaties and the one in general international law (ibid, para. 90).

But then, when it reaches the bottom line of its reasoning, none of this seems to matter – the Court endorses an exceptionally broad approach to the extraterritorial applicability of the ACHR in the environmental context:

The obligations to respect and to ensure human rights require that states abstain from preventing or hindering other States Parties from complying with the obligations derived from the Convention. Activities undertaken within the jurisdiction of a State Party should not deprive another State of the ability to ensure that the persons within its jurisdiction may enjoy and exercise their rights under the Convention. The Court considers that states have the obligation to avoid transboundary environmental damage that can affect the human rights of individuals outside their territory. For the purposes of the American Convention, when transboundary damage occurs that affects treaty-based rights, it is understood that the persons whose rights have been violated are under the jurisdiction of the state of origin, if there is a causal link between the act that originated in its territory and the infringement of the human rights of persons outside its territory.

In cases of transboundary damage, the exercise of jurisdiction by a state of origin is based on the understanding that it is the state in whose territory or under whose jurisdiction the activities were carried out that has the effective control over them and is in a position to prevent them from causing transboundary harm that impacts the enjoyment of human rights of persons outside its territory. The potential victims of the negative consequences of such activities are under the jurisdiction of the state of origin for the purposes of the possible responsibility of that state for failing to comply with its obligation to prevent transboundary damage.

(ibid, paras. 101–102)

To put all of this a bit more simply, if, say, a private company operating in Colombia causes transboundary harm to a person located in Ecuador (e.g. by causing pollution), then that person in Ecuador would be within Colombia’s jurisdiction. Although the Court is referring to the effective control of the harmful transboundary activities, it is not saying that the conduct in question has to be attributable to the state, although a fortiori the same reasoning would apply if the emitter of the transboundary harm was a state agent. Rather, all of this is based on the
ability of Colombia, the state of origin, to prevent such harmful acts from occurring (see also ibid, para 104(f)–(h)).

In sum, despite all of the approving references to the jurisprudence of the European Court, the Inter-American Court actually went far beyond anything that its Strasbourg sibling had done. And most importantly for our purposes, whether right or wrong, I also see no plausible way in which this reasoning could be limited to transboundary environmental harms. It can just as easily apply to other types of transboundary harms, such as those to privacy (in the surveillance context) or to other human rights, such as life, health or expression (in the context of cyber operations more generally). If, in other words, a state has the ability to prevent transboundary harms to persons in other states that are caused by non-state actors operating from its territory (e.g. a corporation or a hacktivist group), then the victims of such acts would be within the jurisdiction of the state of origin. And again, a fortiori the same reasoning must apply to surveillance or cyber operations committed by the agents of the state of origin, such as its security services.

The bottom line of the Court’s approach, if applied to surveillance and cyber operations, would be the total elision of any extraterritoriality threshold (not that this is a bad thing). In fact, the Inter-American Court’s key reference to the state’s ability to prevent transboundary harms is redolent of the so-called functional approach to the extraterritorial application of human rights treaties, which was recently endorsed, in a somewhat different context, by the UN Human Rights Committee.

**HRC General Comment no. 36**

The functional approach to extraterritoriality holds that the key question in interpreting the concept of jurisdiction in human rights treaties is not one of state control over the person or over the territory in which the person is located, but one of control over the person’s ability to exercise their human rights. One of the foremost academic proponents of such an approach has been Prof. Yuval Shany (2013), who also happened to be the rapporteur, together with the late Sir Nigel Rodley, on the Human Rights Committee’s 2018 General Comment no. 36 on the right to life (HRC 2018). And here the Committee reframed its previous approach to extraterritoriality, which did look primarily at control over territory or over the victim, and did so precisely in functional terms:

> A state party has an obligation to respect and to ensure the rights under article 6 [ICCPR] of all persons who are within its territory and all persons subject to its jurisdiction, that is, all persons over whose enjoyment of the right to life it exercises power or effective control.

(ibid, para. 63; for the Committee’s prior position, see HRC 2004, para. 10)

As with the Inter-American Court’s advisory opinion, there is no reason of principle why this approach should be confined solely to the right to life. In other words, if correct, the functional approach should apply to all rights in the Covenant to the extent possible. Thus, if a state exercises power or control over an individual’s enjoyment of the right to privacy by subjecting that individual to surveillance, or by processing or disclosing their personal information, the ICCPR should apply. The same goes for cyber operations that would affect other rights, including the right to life. To be clear, the Committee is yet to explicitly say so, but this to me seems to be inescapable consequence of the approach it took regarding the right to life.
This brings us to the final recent development that I wish to examine – the 2020 judgment of the Federal Constitutional Court of Germany in which it held that all extraterritorial surveillance activities conducted by German security services had to respect the privacy guarantees in the German Basic Law, even when such activities are conducted against foreigners (Federal Constitutional Court of Germany 2020, para. 87). This is a rich and detailed judgment, most of which deals with the various substantive aspects of how a surveillance regime needs to operate in order to be compatible with fundamental rights, but I will here deal only with the threshold extraterritoriality question.

The extraterritorial application of a state’s constitution is formally not an identical issue to the extraterritorial applicability of human rights treaties. It is perfectly possible for constitutional instruments and the jurisprudence built upon them to adopt principles that are significantly different from those in international human rights law, even if many of the underlying policy considerations are the same (for an extended analysis, see Milanovic 2011, pp. 61–82 discussing US and Canadian case law; see also Raustiala 2009; Neuman 1991). Yet, the judgment of the Constitutional Court is remarkable in its internationalist, universalist language and ambition. The Court thus affirmed that German state authorities are comprehensively bound by the Basic Law, regardless of where they act, and that this is mandated by the need to protect human dignity, as a universal ideal, from state power (Federal Constitutional Court of Germany 2020, para. 89). The Court further emphasised the need to read fundamental rights under the Basic Law in the context of internationally protected human rights, and in light of the responsibilities of the German people in a united Europe and the world (ibid, paras. 94–95).

The Court is thus explicit that limiting the applicability of the Basic Law to German territory would undermine universal human rights (ibid, para. 96). Interestingly, the Constitutional Court so found while expressly acknowledging that the European Court was yet to clarify how the ECHR would apply to extraterritorial surveillance (ibid, paras. 97–98), and noting that there was nothing to stop the Basic Law from comprehensively applying abroad even if the European Court were to adopt a narrower approach with regard to the ECHR. (ibid, para. 99). Finally, the Constitutional Court rightly noted that the application of the Basic Law abroad was only meant to constrain German public authorities, and that it in no way interfered with the application of the domestic law of the territorial state, imposed any burdens on the organs of the territorial state and did not violate the prohibition of intervention in international law (ibid, paras. 101–103).

Again, if the Court took this approach for extraterritorial surveillance measures by German authorities, it would undoubtedly take the same approach with regard to cyber operations that interfere with rights other than privacy and do so more intensely. While it was explicitly framing its analysis as one of the extraterritorial applicability of domestic fundamental rights, it also directly linked these to human rights as protected by international law, explicitly grounding its analysis in the language of universal human dignity. It moreover did so without referring to the notion of jurisdiction in human rights treaties, which does not appear in the Basic Law, nor to the spatial and personal models of that notion in international case law, but simply chose to bind German authorities comprehensively, without restriction, when they act territorially. And, finally, it seemed to have issued a respectful nudge to the European Court that it should follow its lead, even if it remains far from certain that the Strasbourg Court will do so (see more Reinke 2020; Miller 2020; Çali 2020).

Where should the law go?

It is only appropriate to conclude by looking at where the extraterritoriality case law of human rights bodies should be going with respect to surveillance and cyber operations, and where (and when) it is likely to go. Both the normative and the predictive questions are to my mind...
reasonably clear, the latter somewhat less so than the former. Normatively, human rights bodies should coalesce around an expansive, factual approach to extraterritoriality, both generally and with regard to surveillance and cyber operations specifically, as the German Constitutional Court has done.

This, of course, is easier said than done. The universality impulse is hard to resist – to paraphrase the Human Rights Committee ‘it would be unconscionable to so interpret’ human rights treaties as to permit states parties to perpetrate violations of these treaties on the territory of another state, which it could not perpetrate on its own territory (HRC 1981, para. 12.3). But this impulse is offset by considerations of practicality and effectiveness (see Milanovic 2011, pp. 106–117). These are real concerns, but their proper place is on the merits – on how, rather than on whether, human rights law should substantively govern extraterritorial surveillance and other cyber operations. And it is reasonable to argue, for example, that an extraterritorial regulatory regime should be more flexible than the one the state applies within its territory; if for no other reason, then because it has less capabilities to achieve the legitimate aims it may be pursuing when it is acting outside its territory (see Milanovic 2015, pp. 138–139).4

A couple of further points in that regard. First, the nomenclature is less important than the substance. When it comes to the negative duty to respect human rights, it matters little whether human rights bodies choose to approach this issue by applying the traditional personal model of jurisdiction and allowing it to collapse, or by employing a categorical rule that negative obligations are not territorially restricted, or by using some variant of a functional approach. The bottom line will be the same – that all surveillance and cyber operations conducted by state agents outside the state’s territory will be covered by human rights law.

Second, however, the question of positive obligations is more complex, especially regarding the duty to protect human rights from third parties. Here the differences between the various conceptual approaches become starker. Note, for example, how the German Constitutional Court very carefully said nothing about under what circumstances German authorities would have the duty to protect, under the Basic Law, an individual located outside German territory. Would, for instance, German authorities have a due diligence duty to prevent non-state actors operating from German territory from engaging in conduct that could adversely affect privacy and other rights of individuals outside Germany (see in that regard Milanovic and Schmitt 2020)? We have already seen how the Inter-American Court would seem to answer that question affirmatively.

Under a functional approach, which simply looks at the ability of the state to perform its obligations, the extraterritorial threshold inquiry is elided altogether. Under the approach I have advocated for, positive duties of protection would be limited to individuals within the territorial jurisdiction, primarily in order to make the protective obligation subject to clearer, more bright-line rules. But I am not unhappy with the functional approach to positive obligations if that is where states are willing to go – I am just unsure that they are. A particularly instructive case study in that regard is a scenario in which a state acquires intelligence that an individual’s life is in serious and immediate risk while that individual is outside the state’s territory. Would, in such a scenario, the state in the possession of the intelligence have to, at a minimum, warn the individual concerned of the danger they are in, in order to comply with an extraterritorial duty of protection?5

Third, there are certain argumentative avenues that human rights bodies should avoid. They should not base their extraterritoriality jurisprudence in state control over cyber infrastructure, as suggested in an OHCHR paper (OHCHR 2014, para. 34), simply because many potential human rights violations in this context (e.g. hacking a mobile phone to exfiltrate
private data à la Bezos) require no control whatsoever over infrastructure to implement. They should not base their jurisprudence on discredited concepts such as the European Court’s espace juridique. Above all, they should follow the German Constitutional Court and not base their jurisprudence on the citizenship of the victim, whether as a threshold matter or on the merits, as doing so would be antithetical to universality and human dignity as the core ideas of human rights law (for an extensive discussion, see Milanovic 2015, pp. 87–101; for a discussion in the German context, see Schaller 2018). In short, human rights bodies need to do their utmost to avoid arbitrary line-drawing when no such line-drawing is genuinely sustainable in the long run.

As for the predictive question of whether human rights bodies will in fact adopt an expansive approach, and when they will do so, this is more difficult. Their extraterritoriality jurisprudence has in recent years generally been on an upward trajectory. But whether this trend will continue will depend on numerous attendant circumstances. On a most basic level, cases squarely presenting these issues need to be actually litigated in the relevant forum, with other admissibility issues, most importantly the exhaustion of domestic remedies, being properly taken care of. Similarly, the extraterritorial application of human rights treaties to surveillance and cyber operations is inseparable from other possible state activities, e.g. kinetic uses of force, and human rights bodies will inevitably consider the implications of what they do and try to be reasonably consistent in different categories of cases.

On a bigger picture level, much will depend on the general political climate and on any backlash human rights bodies are subjected to. If that backlash is not catastrophic, eventually they will likely coalesce around a similar, if not identical, approach to extraterritoriality, along the lines that I have suggested above. The known unknown here is the European Court, which has long been the outlier among human rights bodies with its more restrictive extraterritoriality jurisprudence. It is simultaneously the human rights body to which surveillance and cyber cases has and will be brought first, and the one that will do its best to avoid deciding on the extraterritoriality threshold if it does not have to. Thus, for instance, in the Big Brother Watch case that is, as of the time of writing, pending before the Grand Chamber of the Court and that concerns UK surveillance programmes, the extraterritoriality issue will almost certainly be avoided because some of the applicants are UK-based organisations (ECtHR 2018, para. 271).

The Court’s evasiveness cannot, however, last forever. On the one hand, this is because it has numerous other cases before it that present the extraterritoriality issue and that may compel it to depart from Bankovic even more than it has done so far – for instance, the Bankovic-in-reverse interstate case brought by the Netherlands against Russia about the downing of the MH17 airliner over Ukraine (ECtHR 2020). On the other hand, that other European Court – the Court of Justice of the European Union – has been much more courageous in striking down transatlantic data-sharing arrangements that unduly impinge on privacy as US surveillance programmes do not provide sufficient safeguards (European Court of Justice 2020). And let us also not forget the gentle German nudge in that regard. It thus seems to me more likely than not that the Strasbourg Court will eventually join its siblings in adopting a more liberal, expansive and factual approach to extraterritoriality.

One final point: arguing that human rights law applies to extraterritorial surveillance and cyber operations does not turn human rights into some kind of all-encompassing regulatory regime for extraterritorial surveillance and cyber operations. In particular, espionage and cyber operations that are limited to state data or assets (e.g. the exfiltration of military secrets or the sabotage of air defences systems and the like) would normally not engage the human rights of individuals. The legal interest affected is that of the state, and not of any specific individual, and their protection (if any) is a matter for other rules of international law, such
as sovereignty, the prohibition of intervention or the prohibition of the use of force. Conversely, however, it is entirely appropriate for human rights law, focused as it is on protecting individual interests, to operate alongside other parts of international law that appropriately protect state interests.

Notes

1. Thus, under Article 2(1) ICCPR, ‘[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant,’ under Article 1 ECHR ‘[t]he High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention,’ while under Article 1(1) ACHR ‘States Parties to this Convention undertake to respect the rights and freedoms recognized herein and to ensure to all persons subject to their jurisdiction the free and full exercise of those rights and freedoms’.

2. I would personally prefer to deal with such cases on the basis that negative obligations are unrestricted, or under the personal model (which amounts to the same thing), but as noted above they could also potentially be dealt with by a human rights body under the spatial model, even though the person whose rights are being not violated is not actually present in the territory controlled by the state.

3. See HRC (2014) Concluding observations on the fourth periodic report of the United States of America, UN Doc. CCPR/C/USA/CO/4, para. 22 (referring to surveillance ‘both within and outside the United States’); HRC (2015) Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland, UN Doc. CCPR/C/GBR/CO/7, para. 24 (referring to surveillance activities ‘both within and outside the state party’).

4. This is in fact precisely what the German Constitutional Court has said, by holding that the extraterritorial context may warrant differences in applying the proportionality analysis – see Federal Constitutional Court of Germany 2020, para. 104.

5. An issue directly raised in the case of Jamal Khashoggi – see, e.g., Kirkpatrick 2018; for more on the Khashoggi affair, see Callamard 2020; Milanovic 2020.

6. It would be entirely arbitrary, for example, for the ECHR to apply to the UK spying on an individual in Russia but not one in China, simply on the basis that Russia is, like the UK, an ECHR state party. Even the UK’s Investigatory Powers Tribunal thought so – see Investigatory Powers Tribunal 2016, para. 55 referring to the espace juridique concept.

References


_____ (2008) Liberty and Others v. the United Kingdom, Application no. 58243/00.


European Court of Justice (2020) Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, Case C-311/18 (Schrems II).


Marko Milanovic


