4

Toepasselijkheid van EVRM in geval van onderschepping van de communicatie door verdragsstaat

Europees Hof voor de Rechten van de Mens
12 september 2023, 64371/16 en 64407/16,
ECLI:CE:ECHR:2023:0912JUD006437116
(Kucsko-Stadlmayer, Eicke, Vehabović,
Lubarda, Seibert-Fohr, Guerra Martins,
Bormann)
Noot prof. mr. dr. J.J. Oerlemans,
mr. dr. M. Hagens

Aftappen. Elektronische communicatie. Jurisdictie.

[EVRM art. 8]

Het voornaamste punt in deze zaak is de vraag of, voor het doel van een klacht op grond van art. 8 EVRM, personen buiten een aangesloten staat onder de territoriale jurisdictie van het EVRM vallen wanneer hun elektronische communicatie werd (of het risico liep om te worden) onderschept, doorzocht en onderzocht door de inlichtingendiensten van de staat die binnen haar eigen grenzen handelt.
De eerste klager is een IT-professional en een onafhankelijke onderzoeker die in Florida woont. De tweede klager is een privacy- en veiligheidsonderzoeker en de ontwikkelaar van een open source malware analyse systeem die in Berlijn woont. De klagers hebben bij de Investigatory Powers Tribunal (hierna: IPT) verzocht om te achterhalen of inlichtingendiensten in het Verenigd Koninkrijk onrechtmatig hun gegevens hebben verkregen. Het IPT heeft achterhaald dat communicatie vanaf één van haar e-mailadressen werd onderschept en werd gebruikt voor een onderzoek. Het IPT weigerde de klachten verder te behandelen omdat de klagers buiten het Verenigd Koninkrijk wonen.
Volgens het Verenigd Koninkrijk waren de klachten geen rechtsklachten maar waren ze enkel bedoeld om te achterhalen of de inlichtingendiensten informatie over personen of organisaties bezitten. Volgens het Verenigd Koninkrijk vallen de klachten buiten het bereik van art. 1 EVRM. Tenzij een individu aanwezig is in het Verenigd Koninkrijk, is er geen jurisdictie voor het EHRM om te oordelen over een klacht over de onderschepping, verkrijging of omgang met communicatie door de overheid en/of inlichtingendiensten.
Volgens het EHRM is de voornaamste vraag in deze zaak de vraag naar de ontvankelijkheid. Volgens de Engelse overheid zijn hier twee bezwaren tegen: uitputting van nationale rechtsmiddelen en jurisdictie voor de doeleinden in art. 1 EVRM. Volgens klagers was er ten tijde van het nationale besluit van het IPT geen recht van beroep.
De uitoefening van rechtsmacht door een aangesloten staat is een noodzakelijke voorwaarde om aansprakelijk te worden gehouden voor toerekenbare handelingen of nalatigheden die aanleiding geven tot een beschuldiging van schending van de rechten en vrijheden van het EVRM.
Volgens het EHRM heeft de inmenging in de rechten van klagers ingevolge art. 8 EVRM plaatsgevonden binnen het Verenigd Koninkrijk, omdat de communicatie van klagers werd onderschept, onderzocht en gebruikt in het Verenigd Koninkrijk. Daardoor valt de schending van hun rechten binnen de territoriale rechtsmacht van het Verenigd Koninkrijk.

Wieder and Guarnieriv
tegen
het Verenigd Koninkrijk.

Introduction
1. The principal issue to be addressed in the present case is whether, for the purposes of a complaint under Article 8 of the Convention, persons outside a Contracting State fall within its territorial jurisdiction if their electronic communications were (or were at risk of being) intercepted, searched and examined by that State's intelligence agencies operating within its borders.

The facts
2. The applicant in application no. 64371/16 ("the first applicant"), Mr Joshua Wieder, is a national of the United States of America who was born in 1984 and lives in Cloud Lake, Florida. The applicant in application no. 64407/16 ("the second applicant"), Mr Claudio Guarnieri, is an Italian national, who was born in 1987 and lives in Berlin, Germany. Both applicants are represented before

the Court by Mr M. Scott of Bhatt Murphy Solicitors, a lawyer practising in London.
3. The United Kingdom Government were represented by their Agent, Mr J. Gaughan of the Foreign, Commonwealth and Development Office.
4. The Italian Government did not seek to exercise their right to intervene (Article 36 § 1 of the Convention and Rule 44 of the Rules of Court).

The circumstances of the case
5. The facts of the case may be summarised as follows.

A. The applicants
6. The first applicant is an IT professional and independent researcher. He has worked for commercial data centres and news organisations.
7. The second applicant is a privacy and security researcher and the creator of an open source malware analysis system. He has researched and published extensively on privacy and surveillance with Der Spiegel and The Intercept.

B. The Liberty proceedings
8. On 5 December 2014, 6 February 2015 and 22 June 2015 the Investigatory Powers Tribunal ("the IPT") handed down three rulings on an application lodged by ten human rights organisations ("the *Liberty* proceedings": see *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, §§ 28-60, 25 May 2021). That case concerned the bulk interception of communications by the United Kingdom intelligence agencies pursuant to section 8(4) of the Regulation of Investigatory Powers Act 2000 ("RIPA") and the receipt by the United Kingdom intelligence agencies of material intercepted by their foreign counterparts. The IPT upheld the lawfulness of those regimes, finding neither to be in breach of Articles 8, 10 or 14 of the Convention. However, it accepted that prior to disclosures made in the course of the proceedings, "the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or... Upstream, contravened Articles 8 or 10 ECHR". The IPT was of the view that without the disclosures made, there would not have been adequate signposting of the existing arrangements, as was required under Articles 8 and 10 of the Convention.
9. It further held that the communications of one of the applicant organisations had been lawfully and proportionately intercepted and accessed pursuant to section 8(4) of RIPA but that the material had been retained for longer than permitted in breach of Article 8 of the Convention. In respect of another applicant organisation, the IPT found that communications from an email address associated with it had been intercepted and selected for examination under a section 8(4) warrant. Although it was satisfied the interception was lawful and proportionate and that selection for examination was proportionate, the IPT found that the internal procedure for selection had not been followed and consequently there had been a breach of the complainant's Article 8 rights.
10. The IPT made no finding that the communications of any of the complainants in the *Liberty* proceedings had been obtained by US authorities pursuant to Prism and/or Upstream, and unlawfully shared with the United Kingdom.

C. The Privacy International campaign
11. There followed a worldwide campaign by Privacy International, one of the applicants in the *Liberty* proceedings, through which it sought to encourage individuals to lodge complaints with the IPT.
12. The applicants in the present case lodged applications with the IPT with the aid of a standard application form made available on Privacy International's website. They alleged that the respondent Government and/or the security services had breached Articles 8 and 10 of the Convention because they had and/or continued to intercept, solicit, obtain, process, use, store and/or retain their information and/or communications; and because their information and/or communications were accessible to the respondent Government as part of datasets maintained wholly or in part by other Governments' intelligence agencies; and that the Government and/or security services might have acted unlawfully under domestic law by intercepting, soliciting, accessing, obtaining, processing, storing or retaining their information and/or communications in breach of their own internal policies and procedures.
13. Over 600 applications of a similar nature were received by the IPT. Of these complainants, 294 were resident in the United Kingdom.
14. The IPT listed the first ten applications (which included those lodged by the present applicants)

for hearing to enable issues to be addressed as to whether the claims should be investigated. The applicants, together with four other complainants, were represented in the proceedings; the other four complainants were neither represented nor identified, except to the extent that it could be said that three were resident in the United States of America and one was resident in the United Kingdom.

D. The Government's preliminary submissions to the IPT

15. The Government made preliminary submissions to the IPT in which they sought a "principled basis on which the claims generated by the Privacy campaign can be addressed". In the Government's view, these complaints raised no new issues of law but were instead designed for the purpose of finding out whether the intelligence agencies in fact held information about persons or organisations, or whether they had access to that material from the United States' National Security Agency ("NSA"). The operation of the regime had been examined in detail in the *Liberty* proceedings and nothing would be achieved by requiring individual examination of a potentially very large number of cases.

16. Of the first ten claims before the IPT, five of the complainants were resident abroad. The Government argued that these complainants were outside the scope of Article 1 of the Convention and, as such, it would be appropriate for the IPT to dispose of their Convention complaints at a preliminary stage on that basis. While it was accepted, more generally, that individuals of any nationality could bring complaints to the IPT, the Government argued that the IPT was entitled to proceed on the basis that unless an individual was present in the United Kingdom, there was no jurisdiction to consider a complaint under the Convention concerning the interception, obtaining or handling of communications by the Government and/or intelligence agencies.

17. The Government further argued, *inter alia*, that the ten complainants could not claim to be victims of a violation of the Convention because they could not show that due to their personal situation they were potentially at risk of being subject to secret interception measures.

18. The complainants contended that their claims required individual consideration. They further contended that the IPT had jurisdiction over those among them who were resident abroad; and that they all enjoyed "victim" status under the Convention.

E. The IPT judgment

19. Prior to the hearing, the parties agreed that the NSA had a lawful basis for targeted interception pursuant to section 702 of the Foreign Intelligence Surveillance Act 1978 (as amended) ("FISA"), and to Executive Order 12333, pursuant to which PRISM and "Upstream" were lawfully sanctioned for "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information". They also agreed that in order to pursue their statutory objectives, the intelligence agencies needed to share intelligence with foreign Governments. Moreover, for the purpose of the hearing, any information supplied to the United Kingdom Government by the NSA was assumed to have been lawfully obtained.

20. The IPT handed down its judgment on 16 May 2016. At the outset, it noted that, encouraged by the jurisprudence of the Court, it had approached the question of *locus standi* on a very open-minded basis and without requiring from its complainants the kind of arguable case they would need to present a case in the High Court. It therefore concluded that the judgments in the *Liberty* proceedings were not the finishing point but rather the starting point for the potential investigation of any proper individual claims. Just as the complainants in the *Liberty* proceedings, who had established sufficient locus to bring the claim, were entitled, after the legal issues had been decided, to have investigations of their own individual circumstances, so should be the case of any other such complainant who could satisfy the locus requirement. To not look at the individual cases of other complainants who could establish the relevant locus would be contrary to *Roman Zakharov v. Russia* ([GC], no. 47143/06, ECHR 2015) and *Weber and Saravia v. Germany* ((dec.), no. 54934/00, ECHR 2006-XI), and to its own duty under RIPA. Moreover, it would undermine the position adopted in *Kennedy v. the United Kingdom* (no. 26839/05, 18 May 2010), in which the Court approved the role of the IPT to such an extent that in *Roman Zakharov* it was prepared to recognise that in consequence there could be a different approach to locus in claims before it. Therefore, whatever the purpose of Privacy Inter-

national's campaign, the IPT was satisfied that each subsequent application had to be considered on its merits.

21. As for victim status, it considered that the appropriate test was whether the applicants could show that due to their personal situation they were potentially at risk of being subjected to the measures complained of (see *Roman Zakharov*, cited above, § 171). Applying this test, it was persuaded that all six of the represented complainants satisfied it in respect of the section 8(4) regime; and – albeit with a significant element of doubt – that all save for Mr Wieder, who was a US citizen, satisfied it in respect of the receipt of intelligence from the NSA. It did so on the basis that, in addition to the mere assertion – taken from the standard application form on Privacy International's website – that they believed that the authorities "may have unlawfully intercepted, solicited, accessed, obtained, processed, used, stored and/or retained my information and/or communications, whatever the source of that information or communications may be", all six complainants had provided supplemental information, including in relation to these two applicants that Mr Wieder was "an IT professional and independent researcher, again substantially involved in intelligence and security matters" and Mr Guarneri was "an independent privacy and security researcher, materially involved in intelligence matters, living in a Council of Europe state". However, as it did not consider there to be sufficient information on Privacy International's standard application form to demonstrate victim status, it did not consider that the four unrepresented complainants (see paragraph 14 above) had established locus.

22. As to the matter of jurisdiction, the complainants accepted that the issue could be determined under Article 8 and that Article 10 added nothing to their argument. The IPT noted that a State's competence under Article 1 of the Convention was primarily territorial and the exceptions so far recognised by the Court concerned acts of diplomatic and consular agents present on foreign territory, the exercise of control and authority over an individual outside a Contracting State's territory, and the exercise of effective control of an area outside a Contracting State's territory (see *Al-Skeini and Others v. the United Kingdom* [GC], no. 55721/07, §§ 133-142, ECHR 2011). Therefore, in the IPT's view, a Contracting State owed no obligation under Article 8 of the Convention to persons both of whom were situated outside its territory in respect of electronic communications between them which passed through that State. Furthermore, it was not persuaded that a privacy right was a right of action present in the jurisdiction and to find otherwise would be to extend the bounds of the domestic courts' jurisdiction under Article 8 of the Convention.

23. Consequently, the IPT dismissed the claims of Mr Guarnieri and Mr Wieder by reference to the Human Rights Act 1998 ("HRA") on the ground that it had no jurisdiction to examine them. It also dismissed the claims of the three unrepresented complainants who were resident in the United States of America. It accepted, however, that the Government had itself acknowledged that any claims made otherwise than by reference to the HRA could not be resisted on this basis.

24. In light of its findings, the IPT directed inquiries in respect of the six represented applicants, with the exception of the HRA claims by Mr Guarnieri and Mr Wieder, and in respect of any claim by Mr Wieder relating to the receipt of intelligence from the NSA. It also directed that a copy of its judgment be sent to all other complainants, notifying those who were not resident in the United Kingdom that their HRA claims were dismissed for lack of jurisdiction. Finally, it indicated that the complainants resident in the United Kingdom, and the complainants not resident in the United Kingdom in respect of their non-HRA claims, would be notified that their claims would be dismissed as unsustainable pursuant to section 68(4) of RIPA if it did not receive further submissions within twenty-eight days of the date of dispatch of the judgment.

F. Subsequent events

25. On 12 September 2016 the IPT notified the representatives of Mr Guarnieri that it had carefully considered his domestic law complaints and made no determination in his favour. According to the letter:

"Under section 68(4) of [RIPA], when not making a determination in favour of an applicant, the Tribunal is only permitted to inform such a complainant that no determination has been made in his favour.

If no determination is made in favour of the complainant that may mean that there has been no conduct in relation to the complainant by any relevant body which falls within the jurisdiction

of the Tribunal, or that there has been some official activity which is not in contravention of [RIPA]. The provisions of [RIPA] do not allow the Tribunal to disclose whether or not your client is, or has been, of interest to the security, intelligence or law enforcement agencies. Nor is the Tribunal permitted to disclose what evidence it has taken into account in considering your client's complaint."
26. The IPT wrote a similar letter to Mr Wieder on 12 September 2016, informing him that his complaint had been considered in light of all relevant evidence and no determination had been made in his favour.

Relevant legal framework and practice

I. Secret surveillance regimes
27. The relevant domestic law and practice is set out in *Big Brother Watch and Others*, cited above, §§ 61-201.

II. The IPT: jurisdiction, judicial review and appeals
28. Pursuant to section 64(4) of RIPA, the IPT was the appropriate forum for any complaint by a person aggrieved by, *inter alia*, conduct by or on behalf of any of the intelligence agencies which he believed to have taken place in relation to him, his property, communications sent by or to him, or intended for him, or to his use of any postal service, telecommunications service or telecommunication system. Pursuant to section 67(1) and (4)-(5) it was the duty of the IPT to hear and consider any complaint made to it, save where the complaint was frivolous or vexatious, or had been made out of time.
29. At the time the applicants brought their domestic proceedings, section 67(8) of RIPA provided that "[e]xcept to such an extent as the Secretary of State may by order otherwise provide, determinations, awards, orders and other decisions of the [Investigatory Powers] Tribunal (including decisions as to whether they have jurisdiction) shall not be subject to appeal or be liable to be questioned in any court". However, in *R (on the application of Privacy International) v Investigatory Powers Tribunal and others* ([2019] UKSC 22), which was handed down on 15 May 2019, the Supreme Court, by a majority of four votes to three, held that section 67(8) of RIPA did not preclude judicial review of a decision of the IPT. In so doing, it disagreed with the first instance court and the Court of Appeal, both of which had held that section 67(8) did preclude judicial review of a decision of the IPT.
30. In addition, a new section 67A was inserted into RIPA with effect from 31 December 2018 to provide a right of appeal from the IPT to the Court of Appeal of England and Wales, or the Court of Session in Scotland.

III. "A question of trust": report of the investigatory powers review by The Independent Reviewer of Terrorism Legislation ("the Anderson Report")
31. The Independent Reviewer of Terrorism Legislation is a person wholly independent of Government, appointed by the Home Secretary and by the Treasury for a renewable three-year term. He is tasked with reporting to the Home Secretary and to Parliament on the operation of counter-terrorism law in the United Kingdom. These reports are laid before Parliament to inform the public and political debate. The purpose of the Anderson Report, which was both laid before Parliament and published on 11 June 2015, and which was named after David Anderson K.C., the then Independent Reviewer of Terrorism Legislation, was to inform the public and political debate on the threats to the United Kingdom, the capabilities required to combat those threats, the safeguards in place to protect privacy, the challenges of changing technology, issues relating to transparency and oversight, and the case for new or amended legislation (see *Big Brother Watch and Others*, cited above, §§ 150-55).
32. Under the heading "The Global Nature of the Internet", the Anderson Report stated the following:
"The trends outlined above [towards an increasing variety of communication methods, an increasing number of devices and an increasing pace of adoption of new technologies] have resulted in a vast increase in data volumes. One exabyte of data is 500 billion pages of text: by 2015, 76 exabytes of data will travel across the internet every year. However, the infrastructure of the internet means data are not territorially bound.
A network is a group of devices which are linked and so able to communicate with one another. The internet is often described as a 'network of networks', all of which are interconnected. Communications over the internet take place through the adoption of protocols which are standardised

worldwide. A single communication is divided into packets (units of data), which are transmitted separately across multiple networks. They may be routed via different countries as the path of travel followed will be a mix of the quickest or cheapest paths; not necessarily the shortest path. The quickest path will depend upon bandwidth capacity and latency (the amount of data which can be sent through an internet connection and the delay). The result of this method of transmission is increased data flows across borders. For example, an email sent between two persons in the UK may be routed via another country if that is the optimum path for the CSPs [Communications Service Providers] involved. The route taken will also depend on the location of servers. The servers of major email services like Gmail, Yahoo and Hotmail are based outside the UK.

It is estimated that somewhere between 10% and 25% of the world's international telephone and internet traffic transits the UK via underwater fibre optic cables and much of the remaining traffic transits cabling in the US. Whilst the cables are not a recent technological development, having been in use since the 1970s, the amount of data that can be carried has steadily risen. Cables carrying data at a rate of 10 gigabits per second were the norm for most of the 1990s. Data rates of 100 gigabits per second have been available since 2010. By 2014 Google had already invested $300million in 60 terabit (60,000 gigabit) per second fibre optic cables. In 2014, it was reported that researchers in the Netherlands and the USA demonstrated data rates of 225 terabits per second."

33. With regard to the difficulties in attributing online communications, the report stated:

"The infrastructure of the internet can make it difficult to attribute communications to their sender and so offers a 'cloak of anonymity' for communications.

An Internet Protocol [IP] address [IP address] is the identifier for a device on a network. The address may be static or dynamic and is usually written and displayed in the following format: 172.16.254.1 (IPv4 – 32 bits), and 2001:db8:0:1234:0:567:8:1 (IPv6 – 128 bits). IPv6 is the latest version of the Internet Protocol.

(a) Dynamic Host Configuration Protocol is used to allocate IP addresses dynamically to devices connected to a network. For example, CSPs assign an IP address to a router and all devices connected to the router use it to form a private IP network. All the connections from the devices on the private network appear to come from the single IP address assigned to the router by using Network Address Translation. CSPs have a pool of IP addresses which are allocated dynamically in sequence, so that a customer's external IP address will change and different customers will use the same external IP address, but not at the same time.

(b) Network Address Translation is a technique used by CSPs to allow a single IP address to be shared by multiple customers simultaneously, sometimes numbered in the thousands. It became necessary due to a shortage of IPv4 addresses, though things will change as IPv6 is increasingly adopted. DRIPA 2014 mandated the retention of subscriber data for some categories of IP addresses, namely, those which are static and those which are dynamically allocated in sequence. The Counter Terrorism and Security Act 2015 [CTSA 2015] seeks to address the difficulty which arises when IP addresses are shared by a number of users simultaneously, by requiring the retention of 'relevant internet data' in addition to the shared IP address. However those data are not sufficient to resolve IP addresses in all cases (see 9.51 below); and in any event, a CSP can usually only provide details of the person who pays the internet subscription. This is not necessarily the person who was using a device at a particular time.

One problem created by the variety of devices now commonly used was highlighted by submissions to the Review. Smart phones and tablets are often shared by a number of users, such as family members. Each of these users may be accessing different applications. This pattern of usage differs from the traditional use of a mobile phone by one person. In light of this, one service provider suggested that in the future investigations will need to be much more user-specific. IP matching can only help with this to a certain degree.

A further problem for the attribution of communications is that an IP address can be changed by the use of a proxy server so that a communication appears to come from somewhere it does not. A proxy server acts as an intermediary between a device and the internet, changing the IP address from that of the actual sender to that of the proxy server. Many use proxy servers for perfectly legitimate reasons, such as to maintain privacy online. However, some use proxy servers in order to carry

out cyber attacks so that the origin of the attack remains hidden. Often such attacks involve numerous proxies.
Virtual Private Networks [VPN] act in a similar way to proxy servers by changing the IP address from that of the actual sender to one provided by the VPN. In the past, VPNs were primarily used by companies to allow their employees to access resources on the company's network remotely. Increasingly, VPNs are used by individuals to protect their privacy and security online. Unlike proxy servers, VPNs also provide secure communications through encryption. Multi-hop VPNs offer significantly higher degrees of privacy and anonymity online as they route traffic through two or more VPNs.
Multipath TCP is an example of an emerging technology likely to have implications for IP matching. Most mobile devices can access the internet through both WiFi and a mobile phone data connection, utilising one or the other at one time. Technologies such as Multipath TCP will enable the splitting of traffic between these two methods of access, increasing the number of requests that will have to be made for communications data and making the IP matching process more complex.
Mobile Edge Computing is also likely to diminish the quantity of data entering the central network. It brings content closer to the user by moving it from the central network to the edge of networks. The benefits are faster delivery and better quality for the user, for example, less buffering. However, this is likely to mean fewer communications entering the core network and so lesser volumes of data available for collection.
Nomadic wireless technology provides devices with access to an internet connection within a limited area: for example, the localised WiFi Access Points offered by coffee shops in order to encourage custom. Users are transient and access to the internet by a device can only be traced to a timeslot in the specified premises. If the device connects to the internet elsewhere an identifier called a MAC address will recur, however it is possible to change MAC addresses.
The internet provides opportunities for undetected communications:
(a) Anyone can set up an email address or social networking profile using a pseudonym.
(b) Criminal gangs can use gaming consoles to communicate.
(c) Opportunities for covert communications via the internet include the use of internet cafes and hidden web pages (...).
(d) Encryption software, discussed in more detail below, can be used to hide the content of communications.
(e) An instant messaging service called Wickr allows users to send encrypted and self-destructing messages."

Relevant international law and practice

The Council of Europe

The 2015 Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies
34. In this report the Venice Commission made the following observations on the subject of jurisdiction:
"Strategic surveillance is conducted both within the territory of a state and outside it, by units operating from military bases in allied states, embassies or in ships and aircraft on or, respectively, over the high seas. The collection of intelligence on or over the high seas, or in the territory of another state, with that state's permission, will not be in violation of the customary international law norm of non-intervention. However, the case law of the European Court of Human Rights, and the UN Human Rights Committee clarifies that human rights obligations under these treaties can extend to activities conducted wholly extraterritorially. Collection facilities in military bases, or vessels situated outside national territory can thus also be within 'jurisdiction' for states parties to these treaties. In any event, the processing, analysis and communication of this material is clearly within national jurisdiction and is governed both by national law and states' applicable human rights obligations.
... It may be technically possible for an agency in one state (A) remotely to gain access to computers physically situated within the territory of another state (B), and use this access to plant malware on the computer, allowing it to be monitored. This technical capability does not alter the fact that the computer is within the territory of B, and clearly within its criminal and administrative law jurisdiction. Thus, if A plants malware for security/law-enforcement purposes in computers in B,

then this risks violating the norm of non-intervention if it is not done in compliance with B's law (if this is possible under the law of B at all)."

Relevant comparative law and practice

I. Judgment of 19 May 2020 of the Federal Constutional Court (Bundesverfassungsgericht) (1 BVR 2835/17)

35. The complainants in this case were mostly journalists who reported on human rights violations in conflict zones and in authoritarian States. They challenged the amended version of the Federal Intelligence Service Act (*Gesetz über den Bundesnachrichtendienst*) of 2016 as well as the surveillance measures to which they could be subjected pursuant to this legislation. The amendment of the Act created – for the first time – a statutory basis for the Federal Intelligence Service's practice of strategic surveillance of foreign telecommunications. It granted the Federal Intelligence Service powers to access telecommunications transmission routes and networks to collect telecommunications data in order to identify telecommunications that were of interest to the intelligence services by the use of search terms (selectors), other tools of analysis and by a subsequent manual analysis. According to the challenged provisions, data regarding telecommunications involving German nationals or persons within Germany had to be separated from the other data and deleted prior to any further analysis. Although such data could be collected incidentally, it was excluded from examination or use by the Federal Intelligence Service.

36. On the question of territorial jurisdiction, the Constitutional Court held that the fundamental rights of the Basic Law were binding upon the Federal Intelligence Service and the legislator that set out its powers, irrespective of whether the Federal Intelligence Service was operating within Germany or abroad. The protection afforded by Article 10(1) (the fundamental right to the privacy of telecommunications) and the second sentence of Article 5(1) (freedom of the press) also applied to the telecommunications surveillance of foreigners in other countries. According to the Constitutional Court:

" Art. 1(3) [of the Basic Law] provides that German state authority is comprehensively bound by the fundamental rights of the Basic Law. No restrictive requirements that make the binding effect of fundamental rights dependent on a territorial connection with Germany or on the exercise of specific sovereign powers can be inferred from the provision. In any event, this holds true for the fundamental rights at issue in the present case, which, in their dimension as rights against state interference, afford protection against surveillance measures.

According to Art. 1(3) [of the Basic Law], the fundamental rights of the Basic Law bind the legislature, the executive and the judiciary as directly applicable law. The provision does not contain an explicit restriction to German territory.... Rather, the Basic Law's aim to provide comprehensive fundamental rights protection and to place the individual at its centre suggests that fundamental rights ought to provide protection whenever the German state acts and might thereby create a need for protection – irrespective of where and towards whom it does so.

...

German state authority is bound by fundamental rights even in relation to actions taken vis-à-vis foreigners in other countries; this is also in line with Germany's participation in the international community.

...

This link between fundamental rights and human rights guarantees is incompatible with the notion that the applicability of the fundamental rights of the Basic Law ends at the national border, which would exempt German authorities from having to adhere to fundamental rights and human rights when they act abroad vis-à-vis foreigners. Such a notion would run counter to the Basic Law's aim of ensuring that every person is afforded inalienable rights on the basis of international conventions and beyond national borders – including protection from surveillance (cf. Art. 12 of the Universal Declaration of Human Rights, Art. 17(1) of the International Covenant on Civil and Political Rights). Given the realities of internationalised political action and the ever increasing involvement of states beyond their own borders, this would result in a situation where the fundamental rights protection of the Basic Law could not keep up with the expanding scope of action of German state authority and where it might – on the contrary – even be undermined through the interaction of different states. Yet the fact that the state as the politically legitimated and accountable actor is bound by fundamental rights ensures that

fundamental rights protection keeps up with an international extension of state activities.
The European Convention on Human Rights, which constitutes a guideline for the interpretation of fundamental rights, also suggests such an understanding of the scope of the fundamental rights of the Basic Law (...). It has not yet been comprehensively determined to what extent its guarantees apply to actions of the Contracting Parties outside of their own territory. The European Court of Human Rights is mainly guided by the criterion of whether a state exercises effective control over an area outside its own territory; on this basis, it has in many cases affirmed the applicability of Convention rights abroad (cf. in summary ECtHR [GC], *Al-Skeini and Others v. the United Kingdom*, Judgment of 7 July 2011, no. 55721/07, §§ 132 et seq. with further references; cf. also *Aust, Archiv des Völkerrechts* 52 <2014>, p. 375 <394 et seq. > with further references). However, there has been no final determination as to whether protection is afforded against surveillance measures carried out by Contracting Parties in other states."
37. The Constitutional Court noted that at the time the cases of B*ig Brother Watch and Others v. the United Kingdom* and *Centrum för Rättvisa v. Sweden* were pending before the Grand Chamber. It continued:
"Irrespective of the outcome of these proceedings, the European Convention on Human Rights does not stand in the way of the applicability of German fundamental rights abroad. This is because the Convention is an international treaty with its own separate scope of application; no direct inferences can be drawn from it with regard to the scope of fundamental rights protection under the Basic Law. In any case, the Convention does not rule out further-reaching fundamental rights protection by the Contracting Parties (Art. 53 ECHR)."
38. With regard to technological developments, it noted that:
"The developments in information technology have led to a situation where data is shared through global channels, where it is randomly routed via satellite or cable according to technical criteria that have no regard to national borders (...). This makes it possible to intercept a considerable number of foreign communications from within Germany. Moreover, communication in society has become increasingly international. In view of cross-border services, exchanges – both within states and across national borders – between citizens as fundamental rights holders mainly rely on telecommunications services that do not differentiate between domestic and foreign communications (...). Given that, under the current realities of information technology, actions and communication relations of all kinds have become increasingly digital, and given the constant increase in data processing capacities, the possibilities for conducting telecommunications surveillance extend to broad areas of all of civil society, even outside a state's own jurisdiction – just as domestic communications are also subject to surveillance by other states (...).
In light of such developments, an understanding of fundamental rights according to which their protection ended at national borders would deprive holders of fundamental rights of all protection and would result in fundamental rights protection lagging behind the realities of internationalisation ([...]). It could undermine fundamental rights protection in an increasingly important area that is characterised by intrusive state action and where – in the field of security law – fundamental rights are especially significant in general. By contrast, in binding the state as the relevant actor, Art. 1(3) [of the Basic Law] accounts for such novel risks and helps bring them into the general framework of the rule of law that is created by the Basic Law."

II. Case-law from the United States of America

A. United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)

39. The applicant was a Mexican citizen and resident who was believed to be a leader of a drug smuggling organisation. He was apprehended by Mexican police and transported to the United States of America, where he was arrested. Following his arrest, Drug Enforcement Administration agents searched his Mexican residences and seized certain documents. The question for the domestic courts was whether the Fourth Amendment[1] applied to the search and seizure by United

1 The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported

States' agents of property that was owned by a non-resident alien and was located in a foreign country.
40. In a judgment delivered in 1990, the Supreme Court held that the Fourth Amendment did not apply, since its purpose was to protect the people of the United States against arbitrary action by their own Government, and not to restrain the Federal Government's actions against aliens outside United States' territory. It further held that if there had been a constitutional violation in this case, it occurred solely in Mexico, since a Fourth Amendment violation was fully accomplished at the time of an unreasonable governmental intrusion, whether or not the evidence seized was sought for use in a criminal trial.
41. In the later case of *re Terrorist Bombings*, 552 F.3d 157, 171 (2d Cir. 2008) the Court of Appeals extended the principle established in *Verdugo-Urquidez* and concluded that the Warrant Clause of the Fourth Amendment did not apply to the surveillance of United States' citizens abroad.

B. United States of America v. Microsoft Corporation
42. In December 2013 federal law enforcement agents applied to the United States District Court for the Southern District of New York for a warrant requiring Microsoft to disclose all e-mails and other information associated with an account of one of its customers. A Magistrate Judge issued the warrant directing Microsoft to disclose to the Government the contents of a specified e-mail account and all other records or information associated with the account "[t]o the extent that the information... is within [Microsoft's] possession, custody, or control."
43. Microsoft produced the customer's non-content information to the Government as directed. Those data were stored in the United States. However, Microsoft ascertained that, to comply fully with the warrant, it would need to access customer content that it stored and maintained in Ireland and to import those data into the United States for delivery to federal authorities. It declined to do so. Instead, it moved to quash the warrant.
44. The Magistrate Judge denied Microsoft's motion, resting on the legal conclusion that the warrant in question was more akin to a subpoena than a warrant, and that a properly served subpoena would compel production of any material, including customer content, so long as it was stored at premises owned, maintained, controlled, or operated by Microsoft Corporation. The District Court, after a hearing, adopted the Magistrate Judge's reasoning and affirmed his ruling (see *In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.,* 15 F.Supp.3d 466 (SDNY 2014)). Shortly after, the District Court held Microsoft in civil contempt for refusing to comply fully with the warrant.
45. A panel of the Court of Appeals for the Second Circuit reversed the denial of the motion to quash and vacated the civil contempt finding (see *In re Warrant To Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp*., 829 F. 3d 197, 204– 205 (CA2 2016)). It said the following:
"For the reasons that follow, we think that Microsoft has the better of the argument. When, in 1986, Congress passed the Stored Communications Act as part of the broader Electronic Communications Privacy Act, its aim was to protect user privacy in the context of new technology that required a user's interaction with a service provider. Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas. Three decades ago, international boundaries were not so routinely crossed as they are today, when service providers rely on worldwide networks of hardware to satisfy users' 21st–century demands for access and speed and their related, evolving expectations of privacy."
46. It continued:
"The information sought in this case is the content of the electronic communications of a Microsoft customer. The content to be seized is stored in Dublin. The record is silent regarding the citizenship and location of the customer. Although the Act's focus on the customer's privacy might suggest that the customer's actual location or citizenship would be important to the extraterritoriality analysis, it is our view that the invasion of the customer's privacy takes place under the SCA [Stored Communications Act] where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the

by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

government. Because the content subject to the Warrant is located in, and would be seized from, the Dublin data center, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States. (...)."

47. On 23 March 2018, before the case was considered by the Supreme Court, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) was signed into law. The CLOUD Act amended the Stored Communications Act, 18 U. S. C. §2701 et seq., by adding the following provision:

"A [service provider] shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

48. Pursuant to the new law, the Government obtained a new warrant. As no live dispute remained between the parties, the case became moot. Following the Supreme Court's established practice in such cases, on 17 April 2018 the judgment on review was vacated, and the case was remanded to the United States Court of Appeals for the Second Circuit with instructions first to vacate the District Court's contempt finding and its denial of Microsoft's motion to quash, then to direct the District Court to dismiss the case as moot.

C. United States of America v. Agron Hasbajrami, United States Court of Appeals for the Second Circuit, 18 December 2019

49. The appellant was arrested at John F. Kennedy International Airport in September 2011 and charged with attempting to provide material support to a terrorist organisation. After he pleaded guilty, the Government disclosed that certain evidence involved in his arrest and prosecution – primarily electronic communications between the appellant and individuals without ties to the United States and located abroad – had been derived from information obtained by the Government without a warrant pursuant to its warrantless surveillance program under Section 702 of the FISA [Foreign Intelligence Surveillance Act] Amendments Act of 2008. The appellant then withdrew his initial plea and moved to suppress any fruits of the Section 702 surveillance. The District Court denied the motion to suppress. The appellant again pleaded guilty, reserving his right to appeal the District Court's denial of his suppression motion.

50. On appeal the appellant argued *inter alia* that the warrantless surveillance and the collection of his communications violated the Fourth Amendment. For section 702 surveillance the United States Government could not "intentionally target" anyone located in the United States or a "United States person" outside the United States (Title 50 United States Code ("U.S.C.") §§ 1881a(b)(1), (3)). Nor could it target a non-United States person "if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States" (Title 50 U.S.C. § 188la(b)(2)).

51. The Court of Appeals held that the collection of the communications of United States' persons incidental to the lawful surveillance of non-United States persons located abroad did not violate the Fourth Amendment and that, to the extent that the Government's inadvertent targeting of a United States' person led to collection of the appellant's communications, he was not harmed by that collection. Citing *United States v. Verdugo-Urquidez*, 494 U.S. (1990) and *re Terrorist Bombings*, 552 F.3d 157, 171 (2d Cir. 2008), it stated that "the Fourth Amendment does not apply extra territorially to the surveillance of persons abroad, including United States citizens". In its view, "[t]he protections extended by the Fourth Amendment to foreign individuals abroad, if any, are minimal and plainly outweighed by the paramount national interest in preventing foreign attacks on our nation and its people." The court concluded that:

"the government may lawfully collect, without a warrant and pursuant to Section 702, the e-mails of foreign individuals located abroad who reasonably appear to constitute a potential threat to the United States and, once it is lawfully collecting those emails, it does not need to seek a warrant, supported by probable cause, to continue to collect e-mails between that person and other individuals once it is learned that some of those individuals are United States citizens or lawful permanent residents, or are located in the United States."

52. It continued:

"[the appellant and the amici argued] that *Verdugo-Urquidez* does not control the outcome here because Section 702 collection occurs in the United States. Practically speaking, Section 702 surveillance could occur only within the United States, as the agencies can compel only ISPs located in the United States to provide e-mails. But Fourth Amendment doctrine relating to wire or electronic communication does not focus on the location where the communication takes place. *Katz v. United States*, 389 U.S. 347 (1967), the seminal Supreme Court decision on the interception of such communication, holds that a person's privacy interest in his or her communications does not depend on whether the government physically intrudes into a physical space in which that person has a property interest or an expectation of physical privacy. What matters, and what implicates the protection of the Fourth Amendment, is the expectation of privacy in the communications themselves, and therefore a warrant is required to seize even those communications made in a public telephone booth. Conversely, by the same reasoning, a person who does not have a Fourth Amendment-protected privacy interest in his communications, such as a foreign national resident abroad, does not acquire such an interest by reason of the physical location of the intercepting device. At least where the communication is collected essentially in real time as it occurs, the targeted communication, whether conducted over telephone wires or via the internet, occurs in the relevant sense where the person whose calls or e-mails are being intercepted is located, regardless of the location of the means used to intercept it."

The law

I. Joinder of the applications

53. Having regard to the similar subject matter of the applications, the Court finds it appropriate to examine them jointly in a single judgment (Rule 42 § 1 of the Rules of Court).

II. Receipt of intelligence from foreign intelligence agencies

54. In their applications to the Court, the applicants complained under Articles 8 and 10 of the Convention that their electronic communications may have been obtained by virtue of the operation of the regime governing the receipt by the United Kingdom intelligence agencies of material intercepted by their foreign counterparts. However, they subsequently confirmed that, in light of the Court's conclusions in *Big Brother Watch and Others v. the United Kingdom* ([GC], nos. 58170/13 and 2 others, 25 May 2021), they no longer wished to pursue those complaints.

55. The Court does not see any grounds of respect for human rights as set out in Article 37 § 1 *in fine* which would require it to continue the examination of those complaints, which may therefore be struck out pursuant to Article 37 § 1 (a) of the Convention.

III. The bulk interception regime

A. Article 8 of the Convention

56. The applicants complain under Article 8 of the Convention that, as a result of their work and contacts, their communications might have been intercepted, extracted, filtered, stored, analysed and disseminated by the United Kingdom intelligence agencies pursuant to the regime under section 8(4) of the Regulation of Investigatory Powers Act 2000 ("RIPA").

57. Article 8 provides as follows:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. 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 well-being 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."

1. Preliminary remarks

58. In *Big Brother Watch and Others* (cited above) the Court considered the Convention compliance of the bulk interception regime, which was operated pursuant to section 8(4) of RIPA. It identified certain weaknesses in that regime that gave rise to a breach of Article 8 of the Convention. In particular, there was no independent authorisation of section 8(4) warrants, the categories of selectors used to search intercepted communications did not have to be included in the application for a warrant, and selectors linked to an individual were not subject to prior internal authorisation (*ibid.*, §§ 377-82 and 425).

59. Consequently, the principal issue in the present case is not the Convention compliance of that regime, but rather the preliminary question of admissibility of the individual applications. On this point, the Government have raised two preliminary objections: the exhaustion of domestic remedies, within the meaning of Article 35 § 1 of the Convention; and jurisdictional competence for the purposes of Article 1 of the Convention.

2. The Government's preliminary objections

(a) Exhaustion of domestic remedies

(i) The parties' submissions

(α) The Government

60. The Government relied on *R (On the application of Privacy International) v. Investigatory Powers Tribunal and others*, in which the Supreme Court had held that a decision of the Investigatory Powers Tribunal ("IPT") could be judicially reviewed in the High Court for an error of law ([2019] UKSC 22) (see paragraph 29 above). The Government therefore argued that the applicants had not exhausted domestic remedies, within the meaning of Article 35 § 1 of the Convention, because they had not sought to judicially review the decision of the IPT, even though its findings on jurisdiction were a conclusion of law that was plainly capable of being reviewed by the High Court under its supervisory judicial review jurisdiction.

61. The Government acknowledged that the Supreme Court judgment in *Privacy International* was handed down in 2019, after the present applications were lodged with the Court. However, the Supreme Court judgment simply declared what the law had always been in relation to the IPT. Consequently, the applicants could have challenged the IPT's conclusions in 2016, just as Privacy International had done. In this respect, the Government pointed out that Privacy International's judicial review application (which had led to the 2019 judgment of the Supreme Court) had been brought in 2016, and in those proceedings Privacy International had been represented by the same solicitor who was representing the present applicants.

(β) The applicants

62. The applicants, on the other hand, submitted that at the time of the IPT decision in their case, there was no right of appeal and section 67(8) of RIPA purported to exclude the jurisdiction of the High Court to hear a judicial review application of a decision of the IPT. Shortly after the present applications were lodged with the Court, it was held at first instance, and then on appeal to the Court of Appeal, that this was indeed the effect of section 67(8). This position only changed on 15 May 2019, when the Supreme Court held that in at least some circumstances decisions of the IPT were subject to judicial review. Accordingly, at the time the applicants lodged their applications with the Court the decision of the IPT was final.

(ii) The Court's assessment

(α) General principles

63. It is a fundamental feature of the machinery of protection established by the Convention that it is subsidiary to the national systems safeguarding human rights (see *Vučković and Others v. Serbia* (preliminary objection) [GC], nos. 17153/11 and 29 others, § 69, 25 March 2014).

64. States are dispensed from answering before an international body for their acts before they have had an opportunity to put matters right through their own legal system, and those who wish to invoke the supervisory jurisdiction of the Court as concerns complaints against a State are thus obliged to use first the remedies provided by the national legal system (see, among many authorities, *Vučković and Others*, cited above, § 70 and *Akdivar and Others v. Turkey*, 16 September 1996, § 65, *Reports of Judgments and Decisions* 1996-IV).

65. The obligation to exhaust domestic remedies therefore requires an applicant to make normal use of remedies which are available and sufficient in respect of his or her Convention grievances. The existence of the remedies in question must be sufficiently certain not only in theory but in practice, failing which they will lack the requisite accessibility and effectiveness (see *Vučković and Others*, cited above, § 71 and *Akdivar and Others*, cited above, § 66). The exhaustion of domestic remedies is normally determined at the date on which the application is lodged with the Court (*Baumann v. France*, no. 33592/96, § 47, ECHR 2001-V (extracts)).

66. The Court has frequently underlined the need to apply the exhaustion rule with some degree of flexibility and without excessive formalism (see *Vučković and Others*, cited above, § 76 and *Akdivar and Others*, cited above, § 69). It would, for example, be unduly formalistic to require applicants to exhaust a remedy which even the highest court of their country would not oblige them to exhaust (see *D.H. and Others v. the Czech Republic* [GC], no. 57325/00, §§ 117 and 118, ECHR 2007-IV).
67. As regards the burden of proof, it is incumbent on the Government claiming non-exhaustion to satisfy the Court that the remedy was an effective one, available in theory and in practice at the relevant time (see *Vučković and Others*, cited above, § 77 and *Akdivar and Others*, cited above, § 68).

(β) Application of the general principles to the case at hand
68. In the present case the Court is not being called upon to determine whether the applicants were required to exhaust a new remedy which came into being after they lodged their applications with the Court (compare, for example, *Demopoulos and Others v. Turkey* (dec.) [GC], nos. 46113/99 and 7 others, §§ 87-88, ECHR 2010). The Supreme Court judgment in the *Privacy International* case was delivered in 2019, some three years after the IPT decision in the applicants' case, and the Government does not suggest that they could – or should – have sought permission to apply for judicial review at that stage. Rather, the Government contend that the applicants should have brought judicial review proceedings in 2016, after the IPT decision was handed down in their case.
69. In this regard, the Government state that in 2019 the Supreme Court, in the *Privacy International* case, was simply declaring what the law had always been (see paragraph 61 above). However, in 2016 judicial review of an IPT decision appeared to be precluded by section 67(8) of RIPA (see paragraph 29 above). While the Supreme Court eventually held that judicial review was not precluded by this "ouster" clause, there are two important points to note: first of all, the proceedings brought by Privacy International were unsuccessful at first and second instance (see paragraph 62 above); and the Supreme Court judgment was by a majority of four to three (see paragraph 29 above). As such, it is difficult to accept that in 2016 judicial review of an IPT decision was "sufficiently certain" both in theory and in practice as to constitute an accessible and effective remedy for the purposes of Article 35 § 1 of the Convention.
70. In addition, the Court notes that in other applications before it, which were lodged before the Supreme Court judgment in the *Privacy International* case, the Government did not suggest that the applicants had failed to exhaust domestic remedies because they did not seek to judicially review the decision of the IPT (see, for example, *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008, *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010, and *Big Brother Watch and Others*, cited above). If this possibility was "sufficiently certain" even before the 2019 Supreme Court judgment, it is noteworthy that it was not relied on by the respondent Government in the aforementioned cases.
71. In 2016 Privacy International, together with a number of other applicants, lodged an application before the Court which was linked to the case which would eventually be heard by the Supreme Court in 2019. The applicants alleged that their equipment had been subject to interference known as Computer Network Exploitation or Equipment Interference by the United Kingdom Government Communications Headquarters ("GCHQ") and/or the Secret Intelligence Service ("SIS"). That application was declared inadmissible by the Court on the grounds that the applicants had failed to exhaust domestic remedies (see *Privacy International and Others v. the United Kingdom* (dec.), no. 46259/16, §§ 41-48, 7 July 2020). Before the IPT, Privacy International, together with a number of other applicants, had specifically challenged section 5 of the Intelligence Services Act 1994 ("ISA"), which authorised equipment interference, and section 7 of ISA, which concerned acts taking place outside the United Kingdom. Following the proceedings in the IPT, which did not make a determination in the applicants' favour, Privacy International sought a judicial review of its decision insofar as it concerned section 5 of ISA and, in so doing, challenged the "ouster" clause in section 67(8) of RIPA. While the domestic challenge to section 5 of ISA was ongoing, the applicants complained to the Court under Articles 8 and 10 of the Convention about the power under section 7 of ISA. In

finding that they had not exhausted domestic remedies in respect of this complaint, the Court said the following (at § 46):
"As to the necessity of seeking judicial review in the circumstances the Court recalls that extraordinary remedies cannot, as a general rule, be taken into account for the purposes of applying Article 35 § 1 (see *Tucka v. the United Kingdom (No. 1)* (dec.), no. 34586/10, § 15, 18 January 2011 with further references). It also considers that it was not fully clear at the time the applicants made their application to this Court that pursuing a judicial review of the IPT decision was possible. However, it cannot overlook the fact that the first applicant did attempt such proceedings, was successful and that as a result judicial review proceedings concerning the complaint under section 5 of the ISA are currently pending. As those developments concern the same case and one of the applicants as in the present application, in the circumstances the Court does not regard that attempt at judicial review as an extraordinary remedy and concludes it was therefore a remedy to be exhausted by the applicants."
72. The determinative factor was therefore that the ongoing judicial review proceedings concerned the same case, and was brought by one of the same applicants. Having pursued this challenge in respect of section 5 of ISA, there was no good reason for not having done so in respect of section 7 of ISA. However, it is clear from the Court's findings that prior to the judgment of the Supreme Court in *Privacy International*, in its view it was not "fully clear" that an application for judicial review was possible, and as such, a challenge to section 67(8) of RIPA was an "extraordinary remedy" which applicants would not normally be required to exhaust.
73. As the Government have pointed out, it is perhaps surprising that the present applicants, whose solicitor also represented Privacy International in the aforementioned judicial review proceedings, did not seek to challenge the IPT's conclusions in 2016, just as Privacy International was doing (see paragraph 63 above). However, this alone is not sufficient to overcome the fact that the Government have not sufficiently demonstrated that in 2016, when the applicants lodged the present cases before the Court, an application for judicial review of the IPT's decision was sufficiently "certain", either in theory or in practice, as to provide an accessible and available remedy which the applicants were required to exhaust for the purposes of Article 35 § 1 of the Convention. The Government's preliminary objection on this issue is therefore dismissed.

(b) Jurisdiction

(i) The parties' submissions

(α) The Government
74. The Government asserted that the interception of communications by a Contracting State did not fall within that State's jurisdictional competence for the purposes of Article 1 of the Convention when the sender or recipient complaining of a breach of their Article 8 rights was outside the territory of the Contracting State.
75. The Government argued that a State's jurisdiction within the meaning of Article 1 of the Convention was primarily territorial. Any other basis of jurisdiction was exceptional and required special justification in the particular circumstances (see *Banković and Others v. Belgium and Others* (dec.) [GC], no. 52207/99, § 61, ECHR 2001-XII). In *Al-Skeini and Others v. the United Kingdom* [GC], no. 55721/07, §§ 133-42, ECHR 2011 the Grand Chamber had set out three exceptions to the territorial basis of jurisdiction: State agent authority and control; effective control over an area; and the Convention legal space ("*espace juridique*"). The first of these categories was divided into three sub-categories (*Al-Skeini and Others*, cited above, §§ 134-36): acts of diplomatic and consular agents exercising authority and control over others; the exercise of some or all of the public powers normally exercised by the Government of another State, through that Government's consent, invitation or acquiescence; and the use of force by State agents operating extra-territorially. Before the IPT, the applicants had not relied on any of these exceptions, save as to argue that Mr Guarnieri was within the "*espace juridique*" of the Convention. Before the Court, however, they asserted that the respondent Government exercised control over them by intercepting, accessing, extracting, filtering, storing, analysing and disseminating their communications. The Government contested this argument.
76. For the Government, the interception of communications and related communications data would not involve the exercise of authority and control over the individual whose privacy was in-

terfered with. Given that intercepted communications nevertheless continued on to the recipient, GCHQ could not be said to have exercised full authority and control over those communications, much less over the sender or recipient.
77. The Government further argued that neither of the other two exceptions to the territorial basis of jurisdiction applied. As it was common ground that the applicants had not been physically present in the United Kingdom at any relevant point, any interference with their privacy or freedom of expression must have taken place outside the United Kingdom. In this regard, the Government disputed that the interference with the applicants' rights under Article 8 of the Convention was the interception, extraction, filtering, storage, analysis and dissemination of intercepted content and related communications data. For the Government, a person's private life was a matter of personal autonomy. Interferences with, and effects upon, his private life were therefore not abstract concepts which could be separated from the individual, but rather events which happened to the individual. That was so even if the originating cause of the impact or interference took place in a different State. The interference happened to the individual, and thus took place where the individual was located. The applicants' reliance on case-law concerning Article 1 of Protocol No. 1, and Articles 6, 13 and 5 of the Convention (see paragraph 82 below) was misplaced; either the issue of jurisdiction did not arise in those cases, or they were distinguishable on their facts. Having particular regard to the case-law under Article 1 of Protocol No. 1, the Government argued that privacy, private information and freedom of expression were not property and could not therefore amount to a "possession" for the purposes of Article 1 of Protocol No. 1. Similarly, there was no analogy with the Article 6 case-law as the applicants in those cases had chosen to bring proceedings in the respondent State, and therefore voluntarily submitted to those States' jurisdiction.
78. Moreover, neither applicant fell within the "*espace juridique*" exception, as that did not apply to the facts of the case.
79. For the Government, there was nothing absurd about individuals outside the United Kingdom falling outside that State's territorial jurisdiction. On the contrary, it was simply a natural consequence of the territorial nature of jurisdiction. The very fact that the Convention was not universal meant that jurisdictional lines had to be drawn, and some individuals would fall outside those lines. Such an outcome would not lead to the inevitable conclusion that controls over extra-territorial acts were lacking. In the United Kingdom, for example, surveillance was subject to judicial scrutiny and oversight by the Investigatory Powers Commissioner and the IPT regardless of whether surveillance was directed at individuals within or outside the United Kingdom. Individuals outside the United Kingdom were able to complain to the IPT about breaches of the statutory framework, just as these applicants did, and the IPT could in substance address exactly the same issues under domestic law as might have arisen under the Convention.
80. Finally, before the IPT the applicants had argued that the impugned acts had occurred in the territory of the United Kingdom, and, in respect of the exceptions to the territoriality principle, that Mr Guarnieri was within the "espace juridique" of the Convention. Insofar as they now sought to argue that the respondent State had exercised control over them by intercepting, accessing, extracting, filtering, storing, analysing and disseminating their communications, the Government contended that this argument was in truth an attempt to rerun the argument unsuccessfully made in *Banković and Others* (cited above, § 75), namely, that anyone adversely affected by an act imputable to a Contracting State was brought within the jurisdiction of that State for the purposes of Article 1 of the Convention.

(β) The applicants
81. The applicants argued that their communications and/or related communications data fell within the United Kingdom's jurisdiction for the purposes of Article 1 of the Convention. In their opinion, where interception, storage, processing and interrogation of communications was carried out by the Contracting State on its own territory, it fell within its jurisdictional competence for two reasons.
82. First, where a Contracting State intercepted communications and/or related communications data within its own borders, the resulting interference with Convention rights was within that State's jurisdiction, even if the victim was abroad at the moment of interference. For the applicants, this was consistent with the Court's approach to jurisdiction in respect of other Convention rights,

including Article 1 of Protocol No. 1 (see, for example, *Anheuser-Busch Inc. v. Portugal* [GC], no. 73049/01, § 78, ECHR 2007-I; *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland* [GC], no. 45036/98, § 137, ECHR 2005-VI; *Air Canada v. the United Kingdom*, 5 May 1995, § 28, Series A no. 316-A; and *AGOSI v. the United Kingdom*, 24 October 1986, §§ 49 and 51, Series A no. 108), Article 6 (see, for example, *Markovic and Others v. Italy* [GC], no. 1398/03, §§ 54-55, ECHR 2006-XIV), Article 13 (see *Nada v. Switzerland* [GC], no. 10593/08, §§ 120-23, ECHR 2012) and Article 5 (see *Stephens v. Malta (no. 1)*, no. 11956/07, §§ 51-54, 21 April 2009. They argued that the same approach should apply under Article 8 of the Convention; as with the interference with property, when "correspondence" was intercepted, opened, and read by a Contracting State, the interference took place within the jurisdiction of that State. Any other outcome would render Convention rights illusory in practice.

83. Secondly, the applicants contended that the activity fell within the scope of one of the recognised exceptions to territoriality. When a State carried on secret surveillance in its territory it exercised authority and control over the victim whose communications were intercepted. In the United Kingdom, surveillance was carried out with legal authority and the intelligence agencies assumed full control over intercepted communications. There was no principled basis for holding that "State agent authority and control" required physical control and power over individuals abroad.

84. Finally, the applicants submitted that the consequences would be absurd if they were not within the United Kingdom's jurisdiction for the purposes of Article 1 of the Convention merely because they were not present within its territory at the moment when interception occurred. It would mean that Contracting States could conduct mass surveillance of everyone outside their territory, including their own citizens and citizens of all other Council of Europe Contracting States, and share intelligence obtained in respect of those individuals, without complying with any of the safeguards required by Article 8 of the Convention. It would also mean that if the communications of a person habitually resident in the United Kingdom were intercepted while he was temporarily out of the country, and analysed after his return, the State would have jurisdiction in respect of the analysis but not in respect of the original interception. There was no rational basis for this distinction, which made little sense in view of the fact that the proliferation of online communications had deprived national borders of their meaning.

(ii) The third party intervener

85. Media Defence submitted that Article 1 of the Convention should be interpreted in a manner that responded to the challenges of State conduct of cyber operations and the consequential implications for media freedom – namely, the fact that such operations were capable of intercepting journalistic communications and related data that could identify journalists' sources. Modern day journalism routinely involved investigations across multiple jurisdictions and technological developments had strained the legal frameworks designed to protect journalists and the confidentiality of their sources.

86. According to Media Defence, the notion of "State agent authority and control" should not be interpreted so as to give rise to arbitrary distinctions. In their view, there was no difference between State agents overpowering a journalist while he was abroad in order to secure information on his person, and using sophisticated technology to obtain that same information. In both scenarios, the aim and outcome of the operation was the same.

(iii) The Court's assessment

(α) General principles

87. The exercise of jurisdiction is a necessary condition for a Contracting State to be able to be held responsible for acts or omissions imputable to it which give rise to an allegation of the infringement of rights and freedoms set forth in the Convention (see *H.F. and Others v. France*, [GC], nos. 24384/19 and 44234/20, § 184, 14 September 2022 and *Catan and Others v. the Republic of Moldova and Russia* [GC], nos. 43370/04 and 2 others, § 103, ECHR 2012 (extracts), and the references therein). In the recent case of *H.F. and Others v. France* (cited above, §§ 185-88), which concerned a decision by France not to repatriate a number of its nationals who were living in camps in north-eastern Syria, the Grand Chamber identified the following general principles:

"185. As to the meaning to be given to the concept of 'jurisdiction' for the purposes of Article 1 of the Convention, the Court has emphasised that, from the standpoint of public international law, a State's jurisdictional competence is primarily territorial. It is presumed to be exercised normally throughout the territory of the State concerned. In line with Article 31 § 1 of the Vienna Convention on the Law of Treaties of 1969, the Court has interpreted the words 'within their jurisdiction' by ascertaining the ordinary meaning to be given to the phrase in its context and in the light of the object and purpose of the Convention. However, while international law does not exclude a State's extraterritorial exercise of its jurisdiction, the suggested bases of such jurisdiction (including nationality and flag) are, as a general rule, defined and limited by the sovereign territorial rights of the other relevant States. The Court has recognised that, as an exception to the principle of territoriality, acts of the States Parties performed, or producing effects, outside their territories can constitute an exercise of jurisdiction within the meaning of Article 1 of the Convention. In each case, with reference to the specific facts, the Court has assessed whether the existence of special features justifies the finding that the State concerned was exercising jurisdiction extraterritorially (see *M.N. and Others v. Belgium* [(dec.) [GC], no. 3599/18, §§ 98-99 and 101-02, 5 May 2020], and the references therein, and *Georgia v. Russia (II)* [[GC], no. 38263/08, § 82, 21 January 2021])."

(β) Application of the general principles to the facts of the present case

88. To date, the Court has not had the opportunity to consider the question of jurisdiction in the context of a complaint concerning an interference with an applicant's electronic communications. In *Bosak and Others v. Croatia* (nos. 40429/14 and 3 others, 6 June 2019) the Court did not consider whether the interception of the communications of the two applicants who were living in the Netherlands fell within Croatia's jurisdiction for the purposes of Article 1 of the Convention, perhaps because those applicants' telephone conversations were intercepted and recorded by the Croatian authorities on the basis of secret surveillance orders lawfully issued against another applicant, who lived in Croatia and with whom they had been in contact. While the question of jurisdiction was alluded to in *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 72, ECHR 2006-XI and *in Big Brother Watch and Others* (cited above, § 272), in neither case was it necessary to decide the issue.

89. The applicants in the present case have not suggested that they were themselves at any relevant time in the United Kingdom or in an area over which the United Kingdom exercised effective control. Rather, they contend either that the acts complained of – being the interception, extraction, filtering, storage, analysis and dissemination of their communications by the United Kingdom intelligence agencies pursuant to the section 8(4) regime (see paragraph 56 above) – nevertheless fell within the respondent Government's territorial jurisdiction, or, in the alternative, that one of the exceptions to the principle of territoriality applied.

90. In *Big Brother Watch and Others* the Court identified four stages to the bulk interception process: the interception and initial retention of communications and related communications data; the searching of the retained communications and related communications data through the application of specific selectors; the examination of selected communications/related communications data by analysts; and the subsequent retention of data and use of the "final product", including the sharing of data with third parties (ibid, § 325). Although it did not consider that the interception and initial retention constituted a particularly significant interference, in its view the degree of interference with individuals' Article 8 rights increased as the bulk interception process progressed (ibid, § 330). The principal interference with the Article 8 rights of the sender or recipient was therefore the searching, examination and use of the intercepted communications.

91. In the context of the section 8(4) regime each of the steps which constituted an interference with the privacy of electronic communications, being the interception and, more particularly, the searching, examining and subsequent use of those intercepted communications, were carried out by the United Kingdom intelligence agencies acting – to the best of the Court's knowledge – within United Kingdom territory.

92. It is the Government's contention that any interference with the applicants' private lives occasioned by the interception, storage, searching and examination of their electronic communications could not be separated from their person and

would therefore have produced effects only where they themselves were located – that is, outside the territory of the United Kingdom (see paragraph 77 above).
93. However, such an approach is not supported by the case-law of the Court. Although there are important differences between electronic communications, for the purposes of Article 8 of the Convention, and possessions, for the purposes of Article 1 of Protocol No. 1, it is nevertheless the case that an interference with an individual's possessions occurs where the possession is interfered with, rather than where the owner is located (see, for example, *Anheuser-Busch Inc. v. Portugal* [GC], no. 73049/01, ECHR 2007-I). Similarly, in the specific context of Article 8, it could not seriously be suggested that the search of a person's home within a Contracting State would fall outside that State's territorial jurisdiction if the person was abroad when the search took place. While some of the elements of a person's private life (for example, physical integrity) may not readily be separated from his or her physical person, that is not necessarily the case for all such elements. For example, in *Von Hannover v. Germany* (no. 59320/00, ECHR 2004-VI) the Court appeared to accept that the interference with the applicant's private life which flowed from the publication by German magazines of photographs of her took place in Germany, where the photographs had been published and viewed by the magazines' readership (*ibid*., §§ 53 and 76-81), even though the applicant lived in France and had her official residence in Monaco (*ibid*., § 8), and the photographs in question had been taken in Austria, France and Monaco (*ibid*., §§ 11-17). Similarly, in *Arlewin v. Sweden* (no. 22302/10, §§ 63 and 65, 1 March 2016) the Court found that injury to the applicant's privacy and reputation occasioned by the broadcast of a television programme took place in Sweden, where the programme was broadcast, and not in the United Kingdom, where the broadcaster had its head office.
94. Turning to the facts of the case at hand, the interception of communications and the subsequent searching, examination and use of those communications interferes both with the privacy of the sender and/or recipient, and with the privacy of the communications themselves. Under the section 8(4) regime the interference with the privacy of communications clearly takes place where those communications are intercepted, searched, examined and used and the resulting injury to the privacy rights of the sender and/or recipient will also take place there.
95. Accordingly, the Court considers that the interference with the applicants' rights under Article 8 of the Convention took place within the United Kingdom and therefore fell within the territorial jurisdiction of the respondent State. As such, it is not necessary to consider whether any of the exceptions to the territoriality principle are applicable.

(c) Victim status
96. Although the Government have made no objection based on lack of victim status, the Court can examine this question *ex officio*, since it concerns a matter which goes to its jurisdiction (see, for example, *Buzadji v. the Republic of Moldova* [GC], no. 23755/07, § 70, 5 July 2016).
97. In determining victim status the Court must first have regard to the scope of the legislation permitting secret surveillance measures by examining whether applicants could possibly be affected by it, either because they belong to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Where domestic law provides an effective remedy for persons who believe that their communications have been intercepted, such persons may claim to be victims of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if they are able to show that, due to their personal situation, they are potentially at risk of being subjected to such measures (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 171, ECHR 2015).
98. It follows that, in a case such as the present, where domestic law provided a remedy for all persons who believed that their communications had been intercepted (see paragraphs 28-30 above; see also *Big Brother Watch and Others*, cited above, § 271), potential applicants may claim to be a victim of a violation occasioned by the mere existence of the section 8(4) regime only if they are able to substantiate their claim that they belonged to a group of people who could have been directly affected by the surveillance regime, and that, due to their personal situation, their electronic communications were potentially at

risk of being intercepted, stored and searched by the United Kingdom intelligence agencies pursuant to the section 8(4) regime.
99. For the purposes of the Article 8 complaint the level of persuasion necessary to establish victim status cannot be unreasonably high. The section 8(4) regime is a bulk interception regime and communications may be intercepted, stored and searched even if neither the sender nor recipient is of interest to the intelligence agencies. Moreover, the nature of electronic communications is such that the sender will not know which countries his communications passed through *en route* to the recipients, and cannot, therefore, know which States' intelligence agencies might have had the opportunity to intercept them. Nonetheless, as the Convention does not provide for the institution of an *actio popularis* or for a review the relevant law and practice in *abstracto* (see *Roman Zakharov*, cited above, § 164), potential applicants must take steps to substantiate their claim that they were potentially at risk of having their communications intercepted, searched and possibly even examined under the impugned surveillance regime.
100. In the present case, it is not necessary for the Court to give detailed consideration to this question since the IPT, referring to the Court's case-law, expressly accepted that the applicants had victim status in respect of their Article 8 complaint concerning the section 8(4) regime (see paragraph 21 above). The Government did not challenge that finding and Court would therefore accept that the applicants in the present case can claim to be victims of the alleged violation for the purposes of Article 34 of the Convention.

3. Admissibility
101. The complaint under Article 8 of the Convention is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention.
102. The Article 8 complaint must therefore be declared admissible.

4. Merits
103. The Government accepted that there had been a breach of Article 8 of the Convention by virtue only of the respects in which the section 8(4) regime was held by the Grand Chamber in *Big Brother Watch and Others* (cited above) to violate that Article.
104. As the applicants do not contend that there has been any other violation of their rights under Article 8 of the Convention, the Court, for the reasons identified in *Big Brother Watch and Others* (namely, the absence of independent authorisation, the failure to include the categories of selectors in the application for a warrant, and the failure to subject selectors linked to an individual to prior internal authorisation (*ibid*, §§ 377-82)), finds that there has been a violation of that Article.

B. Article 10 of the Convention
105. Under Article 10 of the Convention the applicants made identical complaints to those previously examined under Article 8 concerning the operation of the regime under section 8(4) of RIPA.
106. Article 10 provides as follows:
"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."
107. In *Weber and Saravia* (cited above, §§ 143-46), in the context of strategic interception (which was a pre-cursor of bulk data interception), the Court held that legislation permitting a system for effecting secret surveillance struck at the first applicant's right, in her capacity as a journalist, to freedom of expression as guaranteed by Article 10 § 1 of the Convention. The applicant communicated with persons she wished to interview on subjects which were also the focus of strategic monitoring. According to the Court, there was a danger that her telecommunications for journalistic purposes might be monitored and that her journalistic sources might be either disclosed or

deterred from calling or providing information by telephone. For similar reasons to those set out in respect of Article 8, the transmission of data to other authorities, their destruction and the failure to notify the first applicant of surveillance measures could serve further to impair the confidentiality and protection of information given to her by her sources.

108. The applicants in the present case do not claim to be journalists. Although the first applicant claims to have worked for news organisations (see paragraph 6 above), he has not specified the nature of his work for those organisations. The second applicant claims to have published extensively on privacy and surveillance with Der Spiegel and The Intercept (see paragraph 7 above) but he does not claim that this publishing work required him to communicate with sources, or that there was any danger that those sources could be disclosed or deterred from providing information by virtue of the bulk interception regime.

109. In fact, in their application to the Court the applicants did not make any arguments under Article 10 of the Convention above and beyond those made under Article 8.

110. Consequently, insofar as the applicants seek to argue that a separate issue arises under Article 10, based on the nature of their work, which is distinct from the violation already found in respect of Article 8, the Court does not consider that they have demonstrated that they were victims of the alleged violation since they have not shown that they were communicating for journalistic purposes (see, for example, *Akdeniz and Others v. Turkey*, nos. 41139/15 and 41146/15, §§ 73-75, 4 May 2021). Although the IPT accepted that the applicants had victim status (see paragraph 21 above), and the Government have not raised any objection on this ground, as victim status concerns a matter which goes to the Court's jurisdiction it is not prevented from examining it of its own motion (see paragraph 96 above; see also *Buzadji*, cited above, § 70, and *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13, § 93, 27 June 2017).

111. Accordingly, this complaint may be declared inadmissible pursuant to Article 34 of the Convention.

C. Alleged violation of Article 13 of the Convention read together with Article 8

112. Lastly, the applicants complained under Article 13 read together with Articles 8 and 10 of the Convention that the IPT did not afford them an effective remedy on account of their being resident outside the United Kingdom. However, having regard to the facts of the case, the submissions of the parties, and its findings above, the Court considers that it has examined the main legal questions raised in the present application and that there is no need to give a separate ruling on the admissibility and merits of the above-mentioned complaint (see, among many other authorities, *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* (GC), no. 47848/08, § 156, ECHR 2014, and *Azer Ahmadov v. Azerbaijan*, no. 3409/10, § 79, 22 July 2021).

IV. APPLICATION OF ARTICLE 41 OF THE CONVENTION

113. Article 41 of the Convention provides:

"If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

114. The applicants make no claim in respect of pecuniary or non-pecuniary damages. In this regard, they stated that a public finding of a breach of the Convention would provide just satisfaction. Accordingly, the Court makes no award in respect of pecuniary damage. In so far as any non-pecuniary damage is concerned, it agrees with the applicants that the finding of a violation constitutes sufficient just satisfaction.

B. Costs and expenses

115. The applicants claimed GBP 13,376.00 for the costs and expenses incurred from 22 September 2021 to 16 May 2022 (being the date the claim was submitted) together with the sum of GBP 54,280.00 in respect of "anticipated future costs".

116. The Government argued that the claim for "anticipated future costs" was a claim for costs that had not been incurred. Moreover, in their view the sum was unparticularised and manifestly excessive.

117. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these were actually and necessarily incurred and are reasonable as to quantum. In the present case, while the claim for costs is divided up into "costs incurred" and "anticipated future costs", the fee notes submitted in support would suggest that some of the "anticipated future costs" were in fact incurred in the preparation of the applicants' observations. According to these fee notes, the professional fees of Mr Ben Jaffey KC were GBP 15,882, inclusive of VAT; the professional fees of Mr David Heaton were GBP 670, inclusive of VAT; the professional fees of Ms Gayatryy Sarathy were GBP 10,616, inclusive of VAT; and the professional fees of Ms Sophie Bird were GBP 2,048, inclusive of VAT. The remainder of the claim for costs has not been supported by any fee notes or bills of costs.
118. Regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 33,155 covering costs under all heads for the proceedings before the Court.

For these reasons, the Court, unanimously,
1. *Decides*, to join the applications;
2. *Decides*, to strike out the complaints concerning the receipt of intelligence from foreign intelligence agencies;
3. *Declares*, the complaints under Article 8 of the Convention concerning the regime under section 8(4) of RIPA admissible;
4. *Holds*, that there has been a violation of Article 8 of the Convention in respect of the regime under section 8(4) of RIPA;
5. *Declares*, the complaints under Article 10 of the Convention inadmissible;
6. *Holds*, that there is no need to examine separately the admissibility and merits of the complaints under Article 13 of the Convention read together with Article 8;
7. *Holds*, that the finding of a violation constitutes in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicants;
8. *Holds*,
(a) that the respondent State is to pay the applicants, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amount, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
(i) EUR 33,155 (thirty-three thousand one hundred and fifty-five euros), inclusive of any tax that may be chargeable to them, in respect of costs and expenses;
(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;
9. *Dismisses*, the remainder of the applicants' claim for just satisfaction.

NOOT

1. Inleiding
De belangrijkste vraag in het onderhavige arrest *Wieder en Guarnieri/het Verenigd Koninkrijk* (EHRM 12 september 2023, nrs. 64371/16 en 64407/16, ECLI:CE:ECHR:2023:0912JUD006437116) die door het Europees Hof voor de Rechten van de Mens (EHRM) wordt beantwoord gaat over jurisdictie. Deze vraag is als volgt: *vallen personen buiten een verdragsstaat binnen de territoriale bevoegdheid van die staat, als hun elektronische communicatie werd (of dreigde te worden) onderschept, bewaard, doorzocht en onderzocht door de inlichtingendiensten van die staat die binnen zijn grenzen opereren?* (par. 1). Het korte antwoord daarop is: 'ja' (par. 95).
Bijzonder aan deze uitspraak is niet dat het over bulkinterceptie gaat, want daarover zijn in recente jaren al meerdere uitspraken verschenen. Het EHRM verwijst in deze zaak voor de vaststelling van de schending van art. 8 EVRM zelfs naar de merites van zijn eerdere uitspraak in de zaak *Big Brother Watch e.a./het Verenigd* Koninkrijk. Daar heeft het EHRM hetzelfde bulkinterceptieregime (op basis van de voormalige Regulation of Investigatory Powers Act (RIPA)) al onder de loep genomen en (vanwege het ontbreken van voldoende waarborgen) in strijd met het EVRM geacht (EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./het Verenigd Koninkrijk*), ECLI:CE:ECHR:2021:0525JUD003525208 (*Centrum för Rättvisa/Zweden*), *EHRC-Updates* 2021, m.nt. Hagens en Oerlemans en «JBP» 2021/62, m.nt. Moyakine).

Bijzonder is wel dat het EHRM voor het eerst in een (bulk)interceptie-zaak toekomt aan de jurisdictie-vraag (par. 88). In eerdere interceptie-zaken woonden (één van) de verzoekers (of waren zij aanwezig) ten tijde van de onderschepping van hun telecommunicatie in de betreffende verdragsstaat. In deze zaak waren de verzoekers niet aanwezig in het Verenigd Koninkrijk of een territorium waar het Verenigd Koninkrijk 'effectieve controle' over had (par. 89).
In deze annotatie bespreken we overwegingen van het EHRM over dit jurisdictievraagstuk met betrekking tot bulkinterceptie als inlichtingenmiddel. We beschrijven kort de achtergrond, noemen de belangrijkste overwegingen van het EHRM en plaatsen dat in context van de discussie die hier al jaren over gaande is. Daarnaast beantwoorden we de vraag of deze uitspraak gevolgen heeft voor Nederland ten aanzien van de bijzondere bevoegdheden in de Wet op inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017).

2. Achtergrond

De zaak draait om twee verzoekers, Wieder en Guarnieri, die klachten indienden bij het Investigatory Powers Tribunal (IPT) over de grootschalige onderschepping van communicatie (bulkinterceptie) door Britse inlichtingendiensten. Deze klachten volgden op eerdere Liberty-procedures in 2014 en 2015, waarbij het IPT de praktijk van bulkinterceptie in strijd achtte met art. 8 en art. 10 Europees Verdrag voor de Rechten van de Mens (EVRM) (par. 8). Privacy International startte daarop wereldwijd een campagne om individuen aan te moedigen klachten in te dienen bij het IPT. Dat resulteerde in meer dan 600 klachten, waaronder die van Wieder en Guarnieri (par. 11-13). Het IPT oordeelde echter op 16 mei 2016 dat elke aanvraag op zijn eigen merites beoordeeld moest worden (par. 20). Met betrekking tot Wieder en Guarnieri was het IPT van mening dat de verzoekers voldoende konden aantonen dat zij door hun persoonlijke situatie mogelijk het risico liepen te worden onderworpen aan bulkinterceptie. Naast het gebruik van het standaardformulier van Privacy International met daarin de stelling dat hun communicatie onrechtmatig zou zijn onderschept, hebben zij aan het IPT aanvullende informatie geleverd dat zij op basis van hun persoonlijke omstandigheden een risico liepen dat hun communicatie zou worden onderschept. Daarbij was het relevant dat de heren onafhankelijke onderzoekers waren en in die hoedanigheid in aanzienlijke mate betrokken waren bij aangelegenheden van inlichtingen en nationale veiligheid (par. 21).
Het IPT wees de aanvragen van de verzoekers af vanwege een gebrek aan jurisdictie (par. 22). Wieder is woonachtig in de Verenigde Staten en Guarnieri in Duitsland (met een Italiaanse nationaliteit). Het IPT overwoog dat de reikwijdte van het EVRM primair territoriaal is beperkt. Tot dusver achtte het EHRM volgens het IPT slechts uitzonderingen mogelijk voor zover het handelingen van diplomatieke en consulaire ambtenaren op buitenlands territorium betrof, de uitoefening van controle en gezag over een persoon buiten het grondgebied van een verdragsstaat, en de uitoefening van feitelijk gezag over een gebied buiten het grondgebied van een verdragsstaat (met verwijzing naar EHRM 7 juli 2011, nr. 55721/07, ECLI:CE:ECHR:2011:0707JUD005572107, par. 133-142 (*Al-Skeini e.a./het Verenigd Koninkrijk*)). Daarom was een verdragsstaat volgens het IPT op grond van art. 8 EVRM geen verplichting ten aanzien van de bescherming van het recht op privacy verschuldigd aan personen die zich beiden buiten zijn grondgebied bevonden met betrekking tot elektronische communicatie tussen hen die via die staat verliep. Als gevolg daarvan wees het IPT de claims van Wieder en Guarnieri af.

3. Beslissing van het EHRM

In de procedure bij het EHRM beargumenteerde het Verenigd Koninkrijk – net als het IPT in haar beslissing – dat het onderscheppen van communicatie door een verdragsstaat niet onder de jurisdictie in art. 1 EVRM valt, wanneer de verzender of ontvanger van telecommunicatie die klaagt over een schending van zijn privacyrechten in art. 8 EVRM, zich buiten het grondgebied van de verdragsstaat bevindt (par. 74). De verzoekers in de onderhavige zaak hebben niet aangevoerd dat zij zich op enig relevant tijdstip zelf in het Verenigd Koninkrijk bevonden of in een gebied waarover het Verenigd Koninkrijk daadwerkelijk controle uitoefende. Zij betogen dat de handelingen – te weten het aftappen, extraheren, filteren, opslaan, analyseren en verspreiden van hun communicatie – door de inlichtingendiensten van het Verenigd Koninkrijk niettemin binnen de territoriale bevoegdheid van de verwerende regering vielen, of, subsidiair, dat één van

de uitzonderingen op het territorialiteitsbeginsel van toepassing was (par. 89).
Het EHRM overweegt dat het aftappen van communicatie en het daaropvolgende doorzoeken, onderzoeken en gebruiken van die communicatie zowel met de persoonlijke levenssfeer van de verzender en/of ontvanger, als op het recht op vertrouwelijke communicatie interfereert (met verwijzing naar EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./het Verenigd Koninkrijk*)). De inmenging vindt plaats waar die communicatie wordt afgetapt, doorzocht, onderzocht en gebruikt, en de daaruit voortvloeiende aantasting van de persoonlijke levenssfeer van de afzender en/of ontvanger vindt daar ook plaats (par. 94).
Aangezien het EHRM van oordeel is dat de inmenging in de rechten van verzoekers uit hoofde van art. 8 RIPA plaatsvond in het Verenigd Koninkrijk, valt het ook onder de territoriale bevoegdheid van de verwerende staat. Als zodanig is het niet nodig om na te gaan of één van de uitzonderingen op het territorialiteitsbeginsel van toepassing is (par. 95).
Ten slotte onderzoekt het EHRM ambtshalve de slachtofferstatus van de verzoekers. Het EHRM bevestigt dat – in het geval van een klacht over bulkinterceptie – voor de toepassing van art. 8 EVRM het bewijsniveau om als slachtoffer aangemerkt te worden niet onredelijk hoog kan zijn (par. 99). Het enkele bestaan van wetgeving die bulkinterceptie mogelijk maakt, kan al voldoende zijn om een schending van de rechten van potentiële verzoekers aan te nemen, mits zij voldoen aan de voorwaarde dat: 'they are able to substantiate their claim that they belonged to a group of people who could have been directly affected by the surveillance regime, and that, due to their personal situation, their electronic communications were potentially at risk of being intercepted, stored and searched by the United Kingdom intelligence agencies pursuant to the section 8(4) regime' (par. 98).
Het EHRM overweegt verder dat de regeling van sectie 8(4) van de RIPA een regeling is voor bulkinterceptie. Communicatie kan worden onderschept, opgeslagen en doorzocht, zelfs als de verzender noch de ontvanger in de aandacht staat van de inlichtingendiensten. Bovendien is elektronische communicatie van dien aard dat de verzender niet weet door welke landen zijn communicatie op weg naar de ontvangers is gegaan, en dus ook niet kan weten welke inlichtingendiensten van welke staten de gelegenheid hebben gehad om de communicatie te onderscheppen. Het EHRM overweegt verder dat het EVRM niet voorziet in de instelling van een 'actio popularis' of een beoordeling van de relevante wetgeving en praktijk in abstracto (met verwijzing naar EHRM (GK) 4 december 2024, ECLI:CE:ECHR:2015:1204JUD004714306, «EHRC» 2016/87, m.nt. Hagens, par. 164 (*Roman Zakharov/Rusland*)). De potentiële verzoekers moeten daarom wel stappen ondernemen om hun bewering te staven dat zij mogelijk het risico liepen dat hun communicatie werd afgetapt, doorzocht en mogelijk zelfs onderzocht in het kader van de aangevochten bewakingsregeling (par. 99). In de onderhavige zaak achtte het EHRM het niet nodig deze vraag in detail te onderzoeken, aangezien het IPT de slachtofferstatus van de verzoekers reeds had aanvaard (par. 100). De regering van het Verenigd Koninkrijk heeft deze bevinding niet betwist en daarom aanvaardde het EHRM de slachtofferstatus van de verzoekers (par. 100).

4. Beschouwing arrest: eindelijk duidelijkheid

De belangrijkste verdienste van het EHRM in dit arrest is dat het duidelijk maakt dat de bescherming van het EVRM bij de inzet van (interceptie) bevoegdheden door inlichtingen- en veiligheidsdiensten van verdragstaten ten aanzien van telecommunicatie niet gebonden is aan de locatie van de betrokkene. Lange tijd bleef dit onzeker, onder andere door het standpunt van het Verenigd Koninkrijk in de *Liberty*-zaken en het hiervoor aangehaalde bevestigende arrest van het IPT, en omdat het EHRM in eerdere zaken over (bulk)interceptie niet aan deze kwestie toekwam. Aan die onzekerheid is door deze uitspraak nu een einde gekomen. Wel geldt nog het 'slachtoffervereiste'. Het EHRM heeft op basis van vaste jurisprudentie (in de Grote Kamer-uitspraak in *Roman Zakharov*, hierboven genoemd) geaccepteerd dat het enkele bestaan van een bulkinterceptieregime een schending van de rechten van potentiële verzoekers kan inhouden. Hierbij geldt echter wel de voorwaarde dat verzoekers onderbouwen dat zij tot een bepaalde groep behoren die door dit interceptieregime direct kan worden geraakt en op basis van hun persoonlijke omstandigheden onderbouwen dat ze een risico lopen dat hun elektronische communicatie hiermee

wordt onderschept en verder wordt verwerkt door de inlichtingen- en veiligheidsdiensten. Een kritiekpunt op het arrest is dat het EHRM in zijn redenering dat sprake is van een inbreuk gebruik maakt van een verwarrende vergelijking tussen de bescherming van telecommunicatie op grond van art. 8 EVRM en 'eigendom' in de zin van art. 1 van protocol nr. 1 (par. 93) (zie ook M. Tzanou, 'Bulk transborder surveillance, foreign nationals and the application of ECHR rights: Wieder and Guarnieri v. the UK – A seminar (but underwhelming) judgment', *Strasbourg Observers*, 21 november 2023). De eindconclusie dat de handelingen van het aftappen en verwerken van de communicatie binnen het territorium van het Verenigd Koninkrijk plaatsvindt en de inmenging op de persoonlijke levenssfeer en het recht op vertrouwelijke communicatie daar dan óók plaatsvindt (par. 94-95), vinden wij echter helder en begrijpelijk.

5. Gevolgen voor Nederland?

De Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) maakt voor wat betreft de eisen bij de inzet van bijzondere bevoegdheden geen onderscheid tussen personen binnen de eigen jurisdictie en in het buitenland (*Kamerstukken II* 2016/17, 34588, nr. 3, p. 51). Dat betekent dat voor de toepassing van een bijzondere bevoegdheid, dezelfde eisen gelden, zoals de toets op proportionaliteit en subsidiariteit en de gestelde eisen in de bijzondere bevoegdheid uit de Wiv 2017. Dit geldt dus ook voor de toepassing van de bijzondere bevoegdheden met betrekking tot 'onderzoeksopdrachtgerichte interceptie' (art. 48-50 Wiv 2017). Deze bijzondere bevoegdheid is vergelijkbaar met de toepassing van de bevoegdheid tot bulkinterceptie door de Engelse inlichtingendienst, zoals in *Wieder en Guarnieri*. In de memorie van toelichting op de Wiv 2017 merkt de wetgever over de inbreuk op de persoonlijke levenssfeer van een niet-Nederlander in het buitenland op dat 'een Nederlandse rechter zich niet bevoegd zal achten zich over deze inbreuk uit te spreken, omdat deze zich strikt genomen niet beperkt tot de Nederlandse jurisdictie' (*Kamerstukken II* 2016/17, 34588, nr. 3, p. 51). In die zin brengt de uitspraak hier een nuance op aan. De zaak *Wieder en Guarnieri* laat zien dat een niet-Nederlander in het buitenland wel degelijk een beroep kan doen op niet-naleving van de Wiv 2017 en een inbreuk op art. 8 EVRM, in het geval van bulkinterceptie door de AIVD of de MIVD, voor zover deze dan ook kan aantonen dat hij voldoet aan het slachtoffer-vereiste, en dat een rechtbank dan in beginsel jurisdictie moet aannemen.

prof. mr. dr. J.J. Oerlemans
Bijzonder hoogleraar Inlichtingen en Recht aan de Universiteit Utrecht en universitair docent Strafrecht bij de Universiteit Leiden.

mr. dr. M. Hagens
Senior onderzoeker bij de CTIVD. Deze noot is op persoonlijke titel geschreven.

5

Vergoeding van immateriële schade heeft geen punitief karakter, maar compensatoire functie

Hof van Justitie EU
21 december 2023, C-667/21,
ECLI:EU:C:2023:1022
(Jürimäe, Piçarra, Safjan, Jääskinen, Gavalec)
Noot prof. mr. dr. A.C. Hendriks

Gezondheidsgegevens. Medisch controleorgaan. Immateriële schade.

[AVG art. 5, 6, 9, 32, 82]

Art. 9 lid 2 onder h AVG moet aldus worden uitgelegd dat de daarin neergelegde uitzondering van toepassing is op situaties waarin een medisch controleorgaan gezondheidsgegevens van een van zijn werknemers niet verwerkt in de hoedanigheid van werkgever maar van medische dienst teneinde de arbeidsgeschiktheid van die werknemers te beoordelen, mits de betrokken verwerking voldoet aan de voorwaarden en waarborgen waarin dat punt h en art. 9 lid 3 AVG uitdrukkelijk voorzien.
De verantwoordelijke voor een op art. 9 lid 2 onder h AVG gebaseerde verwerking van gegevens over de gezondheid is krachtens deze bepaling niet verplicht om te waarborgen dat geen enkele collega van de betrokkene toegang heeft tot de gegevens die betrekking hebben op zijn gezond-