Extraterritorial Bulk Surveillance after the German BND Act Judgment

Marcin Rojszczak*

Foreign surveillance as a means of circumventing existing legal safeguards – Different perspectives on the problem of the extraterritorial application of fundamental rights in US and EU legal models – The limited usefulness of effective control tests for establishing the responsibility of states for action taken in cyberspace – Judgment of Bundesverfassungsgericht in the *BND Act* case as an interpretative guideline for the regulation of foreign surveillance in EU member states – Electronic surveillance as a threat to European integration process.

Introduction

A particular type of surveillance is that aimed at gathering information from foreign sources. Its unrestricted use has led to discussion about whether the importance of privacy – consistently highlighted in recent years – has been losing ground when it comes to foreigners.[1] Although, to paraphrase the words of Marko Milanovic, this problem can be reduced to the question 'Do foreigners deserve privacy?',[2] another, equally important issue arises: does the broad, extraterritorial interpretation of fundamental rights guaranteed in democratic countries

*Assistant professor at Warsaw University of Technology, Faculty of Administration and Social Sciences, Poland. Email: marcin.rojszczak@pw.edu.pl.

[1]A. Lubin, '"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance', 18 *Chicago Journal of International Law* (2018) p. 502.

[2]M. Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', 56 *Harvard International Law Journal* (2015) p. 81 at p. 87-101.

European Constitutional Law Review, 17: 53–77, 2021

doi:10.1017/S1574019621000055

not make their constitutions a 'suicide pact'?[3] And as a result, is it possible to reconcile compliance with the rule of law – which respects the universal nature of human rights – with an obvious need to ensure the security of a state's own citizens?

In May 2020, the German Federal Constitutional Court (Bundesverfassungsgericht) issued a landmark judgment in which it determined that certain powers of the Federal Intelligence Service (BND) to carry out foreign-foreign surveillance violated fundamental constitutional rights.[4] This judgment is worth examining for several reasons. Firstly, the Court made a direct reference to the use of purely foreign-foreign surveillance. Secondly, the judgment was issued by the constitutional court of an EU member state, and therefore took into account the European model of protection of fundamental rights, which stems from both EU law and the European Convention on Human Rights. Thirdly, the Court also addressed in detail the problem of international intelligence cooperation and provided guidelines that might help identify a set of legal safeguards to be applied in the case of cross-border data transfer.

Significantly, the case provided yet another example of the Bundesverfassungsgericht dealing with an assessment of the constitutionality of surveillance regulations through its case law. This most recent judgment can be juxtaposed with earlier, equally important, judgments in the cases of the *G10 Act* of 1999[5] and the *BKA Act* of 2016,[6] which makes it possible to trace the interpretation of constitutional provisions with regard to the state's surveillance powers.

The purpose of this article is to discuss the main conclusions of the *BND Act* judgment from the perspective of transatlantic discussion on the permissible limits of foreign electronic intelligence activities. Therefore, considerable attention will be paid not only to presenting the facts of the case and the judgment, but also to placing considerations concerning the Bundesverfassungsgericht's position in a broader, supranational context. In the first place, in order to make this analysis possible, the first two sections of this work set out the main differences between domestic and foreign surveillance, as well as the key terms used with reference to electronic surveillance. This will be followed by a summary of views on the problem of regulating foreign intelligence activities from the perspective of

[3]R.A. Posner, *Not a Suicide Pact: the Constitution in a Time of National Emergency* (Oxford University Press 2006). Posner's views can be contrasted with position of Koen Lenaerts, President of the Court of Justice of the European Union, according to whom 'the concept of the essence of a fundamental right (...) operates as a constant reminder that our core values as Europeans are absolute. In other words, they are not up for balancing': K. Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU', 20 *German Law Journal* (2019) p. 779.

[4]BVerfG 19 May 2020, 1 BvR 2835/17.

[5]BVerfG 14 July 1999, 1 BvR 2226/94 - 1 BvR 2420/95 - 1 BvR 2437/95.

[6]BVerfG 20 April 2016, 1 BvR 966/09 - 1 BvR 1140/09.

both the US and EU legal models. The discussion of the *BND Act* judgment will be presented in the penultimate section, and its possible impact on European law in the last one.

Domestic versus foreign surveillance in the digital era

The legal systems of most democratic countries have introduced clear restrictions on the admissibility of the activities of foreign intelligence services in their own country. These restrictions are intended to prevent the use of extensive powers in a way that is incompatible with their intended purpose. Foreign intelligence agencies do not conduct criminal proceedings and, as a result, are not bound by the rules that govern these proceedings. Their main objectives are to collect information and provide analyses, as well as anticipate and counteract external threats.

As a result, in democratic countries, the mechanisms used in the areas of domestic and foreign surveillance, although often based on the same technical capabilities, are limited by diametrically opposed legal safeguards. In the case of domestic surveillance, especially conducted as part of criminal procedure, the actions of public authorities need to comply with the principles of subsidiarity, proportionality and strict necessity. Domestic surveillance is also subject to oversight by independent bodies, and individuals subjected to it have legal remedies at their disposal.[7] However, most of these safeguards do not apply in the case of foreign surveillance. As a result, foreign intelligence has for years been an area where the principles of a democratic state have been applied less conscientiously.

Over the last decade, the issue of 'overly extensive surveillance powers' has become a focus of attention for both the public and the scientific community. It has also become a subject of consideration by both constitutional courts and supranational courts. In this regard, particular importance should be attached to the case law of the European Court of Human Rights. The Court has not only developed its own standards for the assessment of national surveillance regulations, but has also used them repeatedly to analyse regulations applied in the area of both national security and the fight against crime.[8] In recent

[7] *See generally* Commissioner for Human Rights, *Democratic and effective oversight of national security services* (Council of Europe, 2015).

[8] *See* a summary of European Court of Human Rights case law related to mass surveillance and national security clause: 'Mass Surveillance – Factsheet', European Court of Human Rights Press Unit, September 2020, ⟨www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf⟩, visited 4 March 2021; 'National security and European case law', European Court of Human Rights, November 2013, ⟨www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf⟩, visited 4 March 2021.

years, the problem of overly extensive surveillance measures taken by public authorities has also been increasingly addressed by the European Court of Justice.[9]

However, in the case of both European Courts, the problem of surveillance powers has been considered mainly in terms of the negative obligations of the state to refrain from arbitrary interference with the rights of individuals. In other words, in the cases examined, the state applied surveillance measures directly or indirectly to persons under its jurisdiction (so-called *domestic-domestic* or *domestic-foreign* surveillance). Clearly, the scope of such surveillance includes the observation of a country's own citizens (including those residing abroad), as well as persons without this status who are in the area of national jurisdiction of a given state or come into contact with its citizens. Therefore, the surveillance of foreign nationals not subject to the jurisdiction of the country that applies the measure (so-called *foreign-foreign* surveillance) fell outside the ambit of judicial authorities' analyses.

The dynamic development of both surveillance regulations and technical possibilities has led to a gradual blurring of the border between surveillance programmes that involve a national link and those of a fully foreign nature. There are two main reasons for this. Firstly, in the age of globalisation the very concept of a 'national link' is difficult to define. Clearly, in the case of traditional telephone calls the geographical location of subscribers can be determined relatively simply (e.g. based on the records of the calls); however this ability is no longer straightforward if the same call is made with the use of a VoIP service. Secondly, the increase in technical capabilities has led to closer international intelligence cooperation. Data intercepted in one country can now be quickly shared with foreign partners. As a result, the country that originally collected the information can pass it on to the intelligence services of another country, which a particular person may also have a link with, for example, in the form of citizenship or place of residence.[10]

[9]Of particular interest are recent judgments in the *Privacy International* (C-623/17) and *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18) cases, in which the Luxembourg Court ruled that a general obligation to retain data is incompatible with EU law, even when this measure is adopted in order to achieve national security purposes. However, it should be noted that the Court per se did not assess the action undertaken by public authorities (this is beyond the jurisdiction of the Court; *see* Art. 276 of the TFEU), but assessed the compliance with EU law of national regulations imposing the obligation to store and share telecommunications metadata on private entities (telecommunications operators).

[10]*See* e.g. H. Gude et al., 'Transfers from Germany Aid US Surveillance', *Spiegel* 5 August 2013, ⟨cli.re/jkaRVk⟩, visited 4 March 2021.

Basic concepts of electronic surveillance

Traditionally, electronic surveillance measures have been divided into targeted and untargeted ones. In the case of targeted surveillance, the authorised bodies are focused on gathering information about specific individuals from the very beginning. Even if it is not possible to identify those persons when initiating the procedures, other selectors (search terms) may be used to limit the scope of surveillance measures. Targeted surveillance has traditionally been associated with the action of law enforcement agencies and the conduct of criminal proceedings, where measures of this kind are applied with external oversight and the legitimacy of the entire process is subject to subsequent review in the course of criminal proceedings.

While targeted surveillance is generally used by law enforcement agencies, untargeted surveillance (often referred to as 'mass' or 'bulk' surveillance) is the domain of security and intelligence agencies. This is due to the simple fact that untargeted surveillance is from the outset geared towards collecting all available information that may be useful. This 'usefulness' should in no way be linked to the 'necessity' of gathering this information and the proportionality of the action taken.[11]

In practice, it is increasingly difficult to identify clear criteria for dividing surveillance techniques into targeted and untargeted ones. This problem has also been the subject of analysis relating to the activities of German intelligence.[12] For several decades, the BND has been monitoring international communication with the use of infrastructure located on German territory in order to gather information and counter serious threats to national security.[13] The Strasbourg Court has recognised that this type of surveillance – referred to as 'strategic

[11]Bulk surveillance is considered a measure that cannot per se be reconciled with the principle of proportionality; it is based on the collection of redundant data, the need for which cannot be demonstrated – and therefore assessed – before these data are recorded. In this regard, Frank La Rue, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, rightly pointed out that: 'Mass interception technology eradicates any considerations of proportionality (. . .). It enables the State to copy and monitor every single act of communication in a particular country or area, without gaining authorization for each individual case of interception' (A/HRC/23/40, p. 16).

[12]*See generally* K. Gärditz, 'Legal Restraints on the Extraterritorial Activities of Germany's Intelligence Services', in R.A. Miller (ed.), *Privacy and Power* (Cambridge University Press 2017) p. 401–34; C. Schaller, 'Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden', 19 *German Law Journal* (2018) p. 941.

[13]An example is the interception of transmissions sent through one of Europe's largest internet exchange points, located in Frankfurt (DE-CIX): A. Meister, 'How the German Foreign Intelligence Agency BND tapped the Internet Exchange Point DE-CIX in Frankfurt, since 2009', *Netzpolitik.org*, 31 March 2015, ⟨cli.re/B5qD5b⟩, visited 4 March 2021.

surveillance' – does not affect obligations arising from the European Convention.[14] Strategic surveillance is, of course, a form of bulk surveillance, so it is not surprising that the Court's position has been cited over the years as evidence that this form of surveillance can – at least to some extent – be reconciled with the requirements of human rights systems. It should be recalled, however, that this judgment was delivered more than 15 years ago and concerned surveillance regulations applied in Germany during the 1990s. The bulk interception of communications at that time was much narrower in scope, both in terms of the types of information collected and its size.

Different perspectives on the extraterritorial application of fundamental rights

Placing *foreign-foreign* surveillance within existing legal frameworks applied in the area of national surveillance requires two basic issues to be resolved. The first is whether this type of activity by public authorities is subject to any restrictions based on a need to respect the fundamental rights of foreigners. Only a positive answer to this question will make it possible to define the source of this obligation and, as a result, to identify the legal safeguards which should apply in this area.

The concept of exterritorial application of constitutional provisions is perceived differently in different legal systems. Excluding undemocratic states and taking into account the scale of surveillance programmes undertaken, it is necessary in the first instance to present American and European doctrines in this field.

The United States

US electronic surveillance programmes are among the most extensive in the world. At the same time it should be borne in mind that both federal and state regulations introduce a number of restrictions on the use of domestic surveillance.[15] However, these restrictions do not apply to foreign programmes, for three main reasons: (i) a lack of recognition of the right to privacy in the catalogue of fundamental rights; (ii) the broad powers of the executive in the area of national

[14]ECtHR 29 June 2006, No 37138/14, *Weber and Saravia* v *Germany*.

[15]Domestic surveillance should be understood here as measures taken by law enforcement agencies as part of criminal proceedings. In the case of US federal legislation, the boundary between domestic and foreign surveillance is in many cases difficult to identify. One reason for this is the very broad definition of 'foreign surveillance' used in the Foreign Intelligence Surveillance Act; another one is the extended interpretation of the so-called *'about'* collection used by the NSA over the years – which refers to cases of domestic communication captured as part of foreign intelligence: L.K. Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age* (Oxford University Press 2016) p. 59-65.

security ; and (iii) the limited effectiveness of human rights treaties in domestic law.

The fundamental source of the right to privacy in the US Constitution is the Fourth Amendment. However, the Fourth Amendment does not *de facto* define the subjective right of individuals, but rather sets out the duty of the state to refrain from 'unreasonable searches'.[16] Consequently, the Fourth Amendment explicitly refers to the relationship between the citizen and the State and is a source of legal safeguards binding on domestic surveillance. In principle, it applies to American citizens and residents.[17]

As early as 1972, the US Supreme Court, in its landmark judgment in the *Keith* case, ruled that electronic monitoring of national communications within the United States must be carried out subject to the Fourth Amendment.[18] Nevertheless, in its 1990 *Verdugo-Urquidez* judgment, the Supreme Court ruled that the Fourth Amendment did not apply to searches carried out by federal agents with respect to foreign nationals' property located outside the United States.[19] The Court explained that '[n]either the Constitution nor the laws passed in pursuance of it have any force in foreign territory unless in respect of our own citizens'.[20] This view expresses the conviction of US jurisprudence that the real purpose of the Fourth Amendment was not to restrict public authorities, but to protect citizens' rights.[21] In this sense, the protective function of the law must be linked to its applicability. In the opinion of the US Supreme Court, in an area where the state's jurisdiction does not extend, not only is there no need for measures limiting the government's actions, such measures may in fact harm the public interest.[22] A narrow interpretation of the scope of application of the Fourth

[16]For more on the Fourth Amendment and its interpretation in the context of cyberspace activities, *see* L.K. Donohue, 'The Fourth Amendment in a Digital World', 71 *NYU Annual Survey of American Law* (2017) p. 533.

[17]The protection under the Fourth Amendment applies to citizens – regardless of where they are actually located, and to all persons (including foreigners) residing in the territory of the United States. *See* E.A. Corradino, 'The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far?', 57 *Fordham Law Review* (1989) p. 617 at p. 618-19.

[18]US Supreme Court, 407 U.S. 297 (1972), *United States* v *U.S. District Court*.

[19]US Supreme Court, 494 U.S. 259 (1990), *United States* v *Verdugo-Urquidez*.

[20]US Supreme Court, 299 U.S. 304 (1936), *United States* v *Curtiss-Wright Export Corp*; *see also* a review of the Court's jurisprudence in *supra* n. 17 at p. 623.

[21]*See United States* v *Verdugo-Urquidez*, *supra* n. 19, at p. 260: 'The Fourth Amendment's drafting history shows that 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'.

[22]*See United States* v *Verdugo-Urquidez*, *supra* n. 19, at p. 273: 'The result of accepting his claim would have significant and deleterious consequences for the United States in conducting activities beyond its boundaries'.

Amendment, limiting it only to persons who 'are part of a national community or who have otherwise developed sufficient connection with (. . .) the country to be considered part of (. . .) community' leads to the conclusion that the activities of public authorities – including those related to electronic surveillance – carried out in relation to foreigners abroad are not subject to constitutional restrictions. This interpretation of the provisions of the Fourth Amendment has also been confirmed by subsequent case law, in particular the case of *Hernandez* v *Mesa*, in which the Court found that the activities of government representatives carried out on United States territory, but where their effects materialised abroad, did not violate the guarantees of the Fourth Amendment.[23]

When discussing the US legal model, it is necessary to take into account the relatively minor role played by international law in shaping the area of fundamental rights. The United States is a party to the International Covenant on Civil and Political Rights and subject to guarantees regarding the protection of privacy that are laid down in Article 17(1) of the Covenant. As a result, it is also subject to an obligation to refrain from using disproportionate surveillance measures.[24] However, the scope of the Covenant's guarantees, although not limited only to citizens, extends solely to persons 'within the territory and subject to the jurisdiction' of a state party.[25] This interpretation of the Covenant has also been confirmed in general comments from the Human Rights Committee.[26] Although this view has evolved in recent years, and there is an increasing likelihood of an interpretation extending the obligations of states to activities also undertaken abroad,[27] there is as yet no basis for recognising the extraterritorial effect of the Covenant in cases where the state does not exercise effective control over an individual.[28] Moreover, due to the notification of

[23]A. Veneziano, 'Applying the U.S. Constitution Abroad, from the Era of the U.S. Founding to the Modern Age', 46 *Fordham Urban Law Journal* (2019) p. 602 at p. 617.

[24]The relationship between the use of surveillance measures and the need to observe the principle of proportionality was emphasised in, inter alia, the resolution of the UN Human Rights Council of 22 March 2017 (A/HRC/34/L.7/Rev.1).

[25]Art. 2(1) of the Covenant.

[26]Human Rights Committee, 'General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant', U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (26 May 2004), p. 10.

[27]*See* e.g. International Court of Justice, Advisory opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 9 July 2004, para 111. *See also* R. Wilde, 'Human Rights Beyond Borders at the World Court: The Significance of the International Court of Justice's Jurisprudence on the Extraterritorial Application of International Human Rights Law Treaties', 12 *Chinese Journal of International Law* (2013) p. 639.

[28]More about the applicability of the Covenant to regulate foreign surveillance activities can be found in: Milanovic, *supra* n. 2; J.J. Paust, 'Can You Hear Me Now?: Private Communication, National Security, and the Human Rights Disconnect', 15 *Chicago Journal of International Law* (2015) p. 612.

derogation and interpretation clauses by the United States during the process of ratifying the Covenant, its practical value in resolving cases before national courts is limited.[29]

The exclusion of US constitutional provisions and the ineffectiveness of international law, combined with the broad powers of the executive to introduce measures for national security purposes, effectively mean that most legal safeguards established in the area of domestic surveillance (in particular, the constitutional 'probable cause' test) do not apply to foreign-foreign types of surveillance programmes carried out by the US intelligence agencies.[30]

The European Union

Compared to the United States, EU member state institutions of international law are given a much greater role in shaping the standard of human rights protection. A special role in this regard is enjoyed by the Strasbourg Court, which has produced a wealth of case law, although in recent decades the Luxemburg Court has also frequently spoken out on issues concerning the protection of fundamental rights.

At the same time, however, the lack of EU competence in the area of national security should not be ignored – resulting as it does from both the current wording of the national identity clause[31] and from a specific regulation confirming the exclusive competence of member states relating to transnational cooperation in the area of national security.[32] The activities of security and intelligence agencies have also been explicitly excluded from the jurisdiction of the European Court of Justice.[33] Yet the Court has spoken out in areas which do not directly concern the legality of actions taken by public authorities, but refer to the compatibility with EU law of obligations imposed on private entities. One example is the extensive jurisprudence issued in cases regarding the general obligation to retain telecommunications data.[34]

[29]K. Ash, 'U.S. Reservations to the International Covenant on Civil and Political Rights: Credibility Maximization and Global Influence', 3 *Northwestern Journal of International Human Rights* (2005) p. [i]-[xiii]; C. Redgwell, 'US reservations to human rights treaties: all for one and none for all?', in M. Byers and G. Nolte (eds.), *United States Hegemony and the Foundations of International Law* (Cambridge University Press 2003) p. 392-415.

[30]D. Severson, 'American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change', 56 *Harvard International Law Journal* (2015) p. 465.

[31]Art. 4(2) TEU: 'National security remains the sole responsibility of each Member State'.

[32]Art. 73 TFEU.

[33]Art. 276 TFEU.

[34]Data retention was a measure originally established during the harmonisation of national laws, and it was only later considered in terms of the approximation of criminal laws. The most recent cases brought before the Court treat data retention as a mechanism used in the area of national security to provide security and intelligence agencies with information for the purposes of electronic surveillance programmes. *See also supra* n. 9.

The case law of the European Court of Human Rights can have a much greater impact on member states' national law applied in the area of surveillance. The scope of European Convention guarantees is not excluded from the area of national security, which is why the Strasbourg Court has the competence to assess the compliance of both national and foreign surveillance programmes with human rights standards. At the same time however, the vast majority of judgments by which the Court has developed its own standard for assessing surveillance provisions concern cases of domestic surveillance.[35] Only three cases explicitly cover the use of foreign surveillance. The first of these judgments, related to BND-led programmes, was handed down in 2006.[36] The other two cases, concerning the assessment of UK[37] and Swedish[38] surveillance programmes, were resolved in 2018, though these judgments are not yet final.

In the German case, the Court did not explicitly address the problem of the legality of foreign surveillance. According to current terminology, however, this case relates more to 'international surveillance' (that is, a *domestic-foreign* one, not of a purely foreign nature). In examining the case, the Court did not address the extraterritorial application of the European Convention, in particular the issue of whether the obligations imposed on states in relation to respect for the rights of individuals also cover foreigners located in third countries. In earlier judgments the Court made it clear that 'the Convention is a multi-lateral treaty operating (. . .) in an essentially regional context and notably in the legal space of the Contracting States. (. . .) The Convention was not designed to be applied throughout the world, even in respect of the conduct of Contracting States'.[39] The issue of cross-border use of surveillance was – albeit only partly – addressed in the *Big Brother Watch and Others* v *the United Kingdom* case, where the Court accepted that the interception of foreign electronic communications fell under the jurisdiction of the United Kingdom and therefore under the obligations laid down in the Convention.[40] This view, if supported by the Grand Chamber[41] and

[35]An example is ECtHR 6 September 1978, No. 5029/71, *Klass* v *Germany*, in which the Court clearly referred to the Convention's scope of application as determined by the state's area of jurisdiction.

[36]*See supra* n. 14.

[37]ECtHR 13 September 2018, Nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch and Others* v *United Kingdom*.

[38]ECtHR 13 June 2018, No. 35252/08, *Centre för Rättvis* v *Sweden*.

[39]ECtHR 10 May 2001, No. 52207/99, *Banković and Others* v *Belgium and Others*, para. 80; but *cf* ECtHR 7 July 2011, No. 55721/07, *Al-Skeini and Others* v *the United Kingdom*, para. 142.

[40]*Big Brother Watch* case, *supra* n. 37, para. 271.

[41]On 4 February 2019, the *Big Brother Watch* case was referred to the Grand Chamber. Similarly, the judgment in another case, *Centrum för Rättvisa* v *Sweden*, also concerning the compliance of national surveillance laws with the Charter, is not yet final, and is pending examination by the Grand Chamber.

developed in subsequent judgments, could affect the interpretation of the European Convention on Human Rights' scope in relation to extraterritorial events. In case law to date, the Court has used the criterions of 'effective control'[42] as a condition of the state's responsibility for actions taken outside its territory.[43]

Hence, the jurisprudence of the European Courts to date does not contain an unambiguous interpretation of whether – and if yes, how – obligations to respect fundamental rights should be met by states in foreign bulk surveillance operations.[44] But given the crucial function of human rights systems in promoting and supporting action in the area of fundamental rights, it is difficult to reasonably assume that the negative obligations of states (to refrain from arbitrary interference) could be completely disregarded with reference to action taken against foreigners located in third countries.

Such a conclusion is supported by analysis of the Strasbourg Court case law regarding the concept of preserving legal space.[45] It applies to cases where a state party to the Convention takes action which results in gaining control of part of another state party's territory. In such a case, in line with the Court's position, all persons under the control of the occupying State should be granted all the rights which they enjoy under the Convention. This would prevent individuals from finding themselves in a 'legal vacuum', where their rights were threatened due to their home country's lack of control over the area in which they resided. Referring the concept of 'preserving the legal space' of electronic surveillance implies that the provisions of the Convention should be applied to programmes

[42]In fact, no single test is applied but rather distinct criterion used to assess the control of a state over an individual and area outside national territory. *See* M. Duttwiler, 'Authority, Control and Jurisdiction in the Extraterritorial Application of the European Convention on Human Rights', 30 *Netherlands Quarterly of Human Rights* (2012) p. 137.

[43]Although the tests of effective control enable the state to be held accountable for events outside its own jurisdiction, they are nevertheless too narrow to be applied to cases of electronic surveillance used in third countries. That is why Peter Margulies proposed a new 'virtual control' test to be applied to the cyber and communication realm. *See* P. Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism', 82 *Fordham Law Review* (2013) p. 2137. For a review of the extensive case law on the extraterritorial application of the Convention, *see* 'Extra-territorial jurisdiction of States Parties to the European Convention on Human Rights', *European Court of Human Rights Press Unit* July 2018, ⟨cli.re/omEN78⟩, visited 4 March 2021. *See also* 'Guide on Article 1 of the European Convention on Human Rights', European Court of Human Rights 2020, ⟨cli.re/JpwmZW⟩, visited 4 March 2021; C. Ryngaert, 'Clarifying the Extraterritorial Application of the European Convention on Human Rights (Al-Skeini v the United Kingdom)', 28 *Utrecht Journal of International and European Law* (2012) p. 57.

[44]D. Cole and F. Fabbrini, 'Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders', 14 *International Journal of Constitutional Law* (2016) p. 220.

[45]*See* ECtHR 10 May 2001, No. 25781/94, *Cyprus* v *Turkey*, para. 78.

carried out with regard to nationals and legal residents of another state party to the Convention, even if these activities are undertaken abroad.

The Bundesverfassungsgericht judgment in the *BND Act* case

In its judgment of 19 May 2020, the Federal Constitutional Court addressed doubts regarding compliance with the fundamental rights of the legal framework for foreign-foreign type bulk surveillance. The Court made it clear that fundamental rights enshrined in the German Constitution were binding not only on German soil – and specifically those activities undertaken by the public authorities – but also in relation to foreigners remaining outside the jurisdiction of the German state. However, this conclusion should not be equated with a need to afford foreigners residing abroad the same protection as their own nationals or foreigners living under the jurisdiction of German law. Moreover, the Court pointed out that, as a rule, the use of bulk surveillance might be a constitutionally justified measure in the area of foreign intelligence – provided that appropriate legal safeguards were applied.[46]

The following sections present the factual background of the case under examination, as well as selected arguments discussed by the Court.[47]

Context of cited case: the BND's surveillance powers

The functioning of the BND in the field of electronic intelligence is governed by two basic laws: the BND Act[48] and the G10 Act.[49] The former defines the general competence of the agency to collect intelligence related to the area of state security.[50] This standard forms the basis for the conduct of foreign electronic intelligence activities. The G10 Act regulates the application of measures interfering

[46]*BND Act* case, *supra* n. 4, para. 154.

[47]*See also* an analysis of the *BND Act* judgment presented in B. Reinke, 'Rights Reaching beyond Borders: A Discussion of the BND-Judgment, dated 19 May 2020, 1 BvR 2835/17', *VerfBlog* 30 May 2020, ⟨cli.re/1kow5X⟩, visited 4 March 2021; R.A. Miller, 'The German Constitutional Court Nixes Foreign Surveillance', *Lawfare*, 27 May 2020, ⟨cli.re/d28ZaB⟩, visited 4 March 2021.

[48]Act on the Federal Intelligence Service (BND-Gesetz – BNDG) [Act on the Federal Intelligence Service], 20 December 1990, BGBl. I p. 2954, 2979, last amended 19 June 2020 (BGBl. I p. 1328).

[49]Act on Restricting the Privacy of Correspondence, Posts, and Telecommunications (Article 10 of the G 10 Act), 26 June 2001, BGBl. I p. 1254, 2298, last amended 19 June 2020 (BGBl. I p. 1328).

[50]*See* Art. 1(2) of the BND Act: '[T]he Federal Intelligence Service collects and evaluates the information required to gain knowledge about foreign countries that are of importance to the Federal Republic of Germany in terms of foreign and security policy'.

with the constitutional right to confidentiality of correspondence and telecommunications – guaranteed in Article 10(1) of the Basic Law (*Grundgesetz*). Therefore, the G10 Act refers to cases of the surveillance of persons under the protection of German constitutional provisions.

In the G10 Act, the German legislature regulated powers and restrictions relating to both targeted[51] and untargeted[52] surveillance. The purpose of targeted surveillance is, amongst other things, to fight against crime, while bulk surveillance (or 'strategic surveillance') aims to gather intelligence and counteract external threats.

The application of strategic surveillance is within the exclusive competence of the BND, and, until the end of the Cold War, its sole purpose was to collect information in order to predict an armed attack on Germany.[53] With the fall of the Berlin Wall, this aim of intelligence activity gradually lost its importance. As a result, the legislature passed an amendment to the regulations in 1994, extending the existing catalogue of tasks carried out within the framework of electronic intelligence to the detection of other serious international threats, such as terrorism, arms trafficking and drug trafficking, as well as money laundering and counterfeiting.[54] The result was a significant extension of the BND's power to collect data not directly related to threats to national security.[55]

The issue of the compatibility of the BND's new powers with the German Constitution was the subject of three constitutional complaints, jointly examined by the Bundesverfassungsgericht in its judgment of 14 July 1999. The Court found that, in principle, strategic surveillance was compatible with the Basic Law,[56] though at the same time pointing to the need to amend a number of specific regulations. In addition, it referred to the problem of whether the activities concerning the collection of foreigners' data were subject to the regime resulting from the G10 Act. Since both the interception and subsequent analysis of the data took place on German territory, the Court found that the process was under the control of the public authorities and

[51]Art. 3(1) of the G10 Act.

[52]Art. 5(1) of the G10 Act.

[53]*G10 Act case*, *supra* n. 5, para. 3. For more on the establishment and early history of the post-war German intelligence service, *see* H.-H. Crome, 'The "Organisation Gehlen" as Pre-History of the *Bundesnachrichtendienst*', 7 *Journal of Intelligence History* (2007) p. 31.

[54]*G10 Act case*, *supra* n. 5, paras. 17-25.

[55]Not every case of combating serious crime is related to national security. The Strasbourg Court referred to this problem by pointing out that drug trafficking – although it is undoubtedly a serious crime – could not be considered a threat to national security in the realities of the case under examination: ECtHR 24 April 2008, No. 1365/07, *C.G. and Others* v *Bulgaria*, para. 43.

[56]*G10 Act case*, *supra* n. 5, para. 194.

within the jurisdiction of national law.[57] As a result, any assessment of its legality had to take into account the proportionality of the interference. Significantly, the Bundesverfassungsgericht explicitly stated that its analysis did not refer to any surveillance other than that regulated under the G10 Act, meaning that foreign-foreign type of surveillance had not been taken into consideration.[58] The compatibility with the fundamental rights of strategic surveillance carried out by the BND became the subject of a complaint to the European Court of Human Rights. In principle the Strasbourg Court supported the line of jurisprudence taken by the Karlsruhe judges, confirming the compatibility of conducting strategic surveillance (based on the provisions of the G10 Act) with the European Convention on Human Rights.[59]

The German authorities have argued for many years that the constitutional guarantees related to the confidentiality of communications do not apply to communications between persons who are not within the jurisdiction of German law.[60] As a result, foreign surveillance programmes were presumed not to be subject to the restrictions of the G10 Act – whether in terms of the purpose of the surveillance carried out, the legal safeguards applied, or the external control of surveillance measures. Although the Bundesverfassungsgericht judgment of 1999 did not predetermine the correctness of such an interpretation, neither did it offer any arguments to show that it was incorrect. As a result, for many years, the operation of such programmes was based solely on internal government and BND regulations.[61]

Another important reform of the BND's powers was carried out in 2016 with the aim of clarifying the provisions of the BND Act, including the scope of tasks to be undertaken by foreign surveillance. The amended regulations also set out the principles for conducting surveillance with regard to public authorities and citizens of other EU member states, the most important of which is the fulfilment of the necessity condition.[62] This criterion has not been defined in relation to the interception of transmissions of non-EU citizens. This is an interesting distinction

[57] *G10 Act case*, *supra* n. 5, para. 176: '(. . .) an act of communication abroad is linked with the action of the state on the domestic territory in such a way that the fundamental rights pursuant to Article 10 of the Basic Law are binding even if it must be supposed, for this binding effect to apply, that the territorial reference must be sufficiently close'.

[58] *G10 Act case*, *supra* n. 5, para. 176.

[59] *See* previous comments on the ECtHR's judgment in *Weber and Saravia* v *Germany* case, *supra* n. 14.

[60] *G10 Act case*, *supra* n. 5, para. 92. *See also* Schaller, *supra* n. 12, at p. 952.

[61] S. Heumann, 'German Exceptionalism?: The Debate About the German Foreign Intelligence Service (BND)', in Miller, *supra* n. 12, p. 349 at p. 367.

[62] Art. 6(3)(3) of the BND Act: 'Search terms which lead to the targeted recording of institutions of the European Union, of public authorities of its member states or of Union citizens may only be used if this is necessary to achieve the goals defined in the cited provision'.

– it shows that the standard of protection of EU citizens' rights introduced by the German legislature is higher than in the case of other foreigners, while at the same time the former have not been granted the same protection enjoyed by persons under German jurisdiction (to whom the G10 Act would apply).[63] Other significant consequences are also linked to the granting of higher protection only to persons with EU citizenship and not to those residing legally in the EU. The scope of application of the new regime under the BND Act does not, therefore, extend to all persons in the EU legal space.

There is no doubt that the shape of the new regulations was influenced by echoes of the US National Security Agency (NSA) surveillance activities revealed by Edward Snowden. One of the topics widely discussed in the media was the cooperation of the BND with its American partner. As a result, the detailed provisions of the BND Act exclude the possibility of carrying out the surveillance of foreigners if the purpose of such activity is economic espionage[64] or the deliberate collection of data on heads of governments of other EU countries.[65]

The amended law also laid down rules for conducting intelligence cooperation with other countries, including criteria for the transfer of data and conditions for the legality of such transfers. A requirement was introduced to formalise this type of cooperation and to obtain external approval for its initiation.[66] The legislature also defined the conditions which must be met for intercepted data to be automatically transferred to foreign intelligence services.[67]

It is worth pointing out that one of the main objectives of this reform seems to have been – rather than equating the legal protection of foreigners and persons under German jurisdiction – to protect the constitutional order by ensuring that the BND's powers would not be used to build a surveillance mechanism that could serve purposes other than those for which the service was established. This is a significant difference, explaining why the amendment to the BND

[63]Art. 6(3)(4) of the BND Act: 'The collection of data from telecommunications traffic from German citizens, from domestic legal entities or from persons residing in the federal territory is not permitted'.

[64]Art. 6(3)(5) of the BND Act. It should be noted that BND has previously been accused of using its powers to conduct economic espionage against European companies, including, reportedly, the Airbus Group. P. Hollinger, 'Airbus files criminal complaint over alleged German spying', *Financial Times* 30 April 2015, ⟨cli.re/KMd28j⟩, visited 4 March 2021. According to data presented by the Parliamentary Control Panel of the German Bundestag, about 3,300 institutions and persons with an EU/NATO link were potentially under surveillance by BND. *See* Schaller, *supra* n. 12, at p. 962.

[65]A. Troianovski and H. Torry, 'German Government Is Accused of Spying on European Allies for NSA', *The Wall Street Journal* 30 April 2015, ⟨cli.re/RABRYn⟩, visited 4 March 2021.

[66]Art. 13(5) of the BND Act.

[67]Art. 15 of the BND Act.

Act does not refer to the concepts of subsidiarity or proportionality as conditions limiting the scope of mass surveillance programmes.

The Bill extending the surveillance powers of the BND was criticised by non-governmental organisations as early as the parliamentary work stage.[68] The basic charges included that overly extensive powers were granted to the BND, and that it provided for the creation of a distinct procedure for managing and controlling surveillance measures, separate from that provided for in the G10 Act. Shortly after the adoption of the new regulations, they were appealed against in the Federal Constitutional Court.[69] The complainants raised three main legal issues: (1) infringement of Article 5(1), to the extent that the new powers of the BND could lead to a violation of the freedom of the press; (2) infringement of Article 10(1), i.e. confidentiality of correspondence; and (3) infringement of Article 3(1), to the extent that the contested provisions could discriminate against EU citizens by granting them a different (lower) level of protection against surveillance from that enjoyed by German residents. Thus, unlike in the *G10 Act Case* of 1999, the key aspect of this complaint was to assess the adequacy of the legal safeguards used in foreign surveillance.

Exterritorial effect of the German Basic Law

The first problem that needed to be resolved by the German Constitutional Court when assessing the legality of foreign surveillance programmes was the possibility of granting foreigners abroad protection arising from fundamental rights guaranteed by domestic constitutional provisions. In its argument, the German Constitutional Court – instead of following the doctrine of effective control over territory or effective control over an individual – presented its own analysis, in which the starting point was the absolute inviolability of human dignity arising from the Basic Law.

Dignity, as a source of other fundamental rights, is of cardinal importance, and is not subject to any restrictions.[70] Christoph Enders sees it not as a kind

[68] J. Nasr and S. Siebold, 'German parliament approves controversial espionage law', *Reuters*, 21 October 2016, ⟨cli.re/4EpRRv⟩, visited 4 March 2021.

[69]'Reporters Without Borders: constitutional complaint lodged against the BND law', *Reporters Without Borders* Press Release, 29 January 2018, ⟨cli.re/kkR21M⟩, visited 4 March 2021.

[70]Art. 1(1) of *Grundgesetz*: 'Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority'. Aharon Barak points out that the adjective 'untouchable' should be used in English translations instead of the commonly used 'inviolable'. In his opinion, 'untouchable' is closer to the German original. In doing so, he also emphasises that human dignity is an absolute right in the German legal order: A. Barak and D. Kayros, *Human Dignity: The Constitutional Value and the Constitutional Right* (Cambridge University Press 2015).

of 'super-basic-right', overriding other fundamental rights, but as a raison d'être.[71] As a result, the Court has recognised in its case law that even public security objectives do not justify the introduction of measures that violate human dignity.[72] Moreover, it has stressed that any law that leads to a violation of dignity must be considered unconstitutional.[73]

According to Article 1(3) of *Grundgesetz*, fundamental rights are directly applicable and binding on all state authorities – executive, legislative and judicial.[74] Against that background, the Court noted that this provision does not introduce any territorial restriction. It is therefore reasonable to conclude that all actions of public authorities are limited by the need to respect fundamental rights, irrespective of whether their effects relate to a person under German jurisdiction or not.[75] The Court pointed out that the interpretation of fundamental rights, as provided for in the German Constitution, cannot disregard the international system of human rights, which is based on the universal recognition of their inviolability and their inalienable nature.[76]

As a result, it was the Court's view that a commitment to the rule of law and democratic model of the state based on respect for human dignity prevents state authorities from respecting only the fundamental rights of persons with German nationality or who are on German territory. At the same time, the Court stressed that this extended application of fundamental rights does not lead to an obligation of public authorities to ensure the protection of individuals who are in foreign jurisdictions. Nor does it limit in any way the sovereign right of other states to freely formulate their domestic law. The extraterritorial effect of fundamental rights guaranteed by the German Constitution imposes an obligation on the public authorities in Germany to respect such rights in all actions they take – including those relating to foreigners residing abroad.[77] In this regard, it is irrelevant whether the state exercises effective control over territory or over an individual.

[71]C. Enders, 'Right to have Rights – The German Constitutional Concept of Human Dignity', 3 *NUJS Law Review* (2010) p. 253 at p. 255.

[72]BVerfG 31 January 1973, 2 BvR 454/71, para. 30.

[73]BVerfG 16 January 1957, 1 BvR 253/56, para. 32.

[74]It is worth recalling that this standard is also applied to the armed forces. In the earlier wording of Art. 1(3), in force before the 1956 amendment to the Basic Law, this provision referred to administrative, legislative and judicial powers. The replacement of 'administrative' with the word 'executive' was connected with the re-establishment of the Bundeswehr and was motivated by a willingness to ensure that all branches of power would be bound by the obligation to respect fundamental rights.

[75]*BND Act* case, *supra* n. 4, para. 89: '[I]n particular, monitoring measures against foreign countries in the forms possible today were beyond the ideas of the time, it cannot be inferred from the history that the protection of fundamental rights a priori should end at the state border'.

[76]*BND Act* case, *supra* n. 4, para. 94.

[77]*BND Act* case, *supra* n. 4, para. 101.

For this reason, it is the opinion of Başak Çali that the type of extra-territorial doctrine that the Bundesverfassungsgericht has applied should be referred to as 'control over the rights of persons'.[78]

Notably, when applying the 'effective control' tests, the state has not only negative but also positive obligations to implement adequate mechanisms to protect the rights of individuals. However, in the case of foreign-foreign surveillance, these obligations apply only to the relationship between the individual and the German state.[79] Nonetheless, it also should be noted that, as Russel A. Miller[80] and David Krebs[81] point out, the *BND Act* judgment may be considered a sanction of the exterritorial applicability of fundamental rights related to scenarios other than electronic surveillance.

Bulk surveillance as a constitutionally justified measure of foreign surveillance

The Federal Constitutional Court determined that the general mechanism established in the amended BND Act – which consisted of creating a separate (and lower) protective regime for the use of foreign surveillance than that based on the G10 Act – was unconstitutional. However, this incompatibility did not result from regulating foreign surveillance differently, but from the establishment of inadequate legal safeguards, which failed to take into account the constitutional standard developed by the Court in its earlier rulings, as well as established case law of the European Court of Human Rights.

In its earlier judgment in the *Census Act* case, the Bundesverfassungsgericht had already ruled that the functioning of the individual in society implies that he or she will tolerate restrictions that arise from the need to protect the public interest.[82] However, this expression of the principle of proportionality is no longer relevant with regard to foreign surveillance. Two questions arise from this: How is the subjection of a foreigner residing abroad to surveillance connected with his or

[78]B. Çali, 'Has "Control over rights doctrine" for extra-territorial jurisdiction come of age? Karlsruhe, too, has spoken, now it's Strasbourg's turn', *EJIL:Talk!* 21 July 2020, ⟨cli.re/DM4aBQ⟩, visited 4 March 2021.

[79]Interestingly, such an interpretation of the scope of application of fundamental rights is almost identical to the conclusions presented in a US Department of State analysis on the geographic scope of the International Covenant on Civil and Political Rights. *See* Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights, Office of the Legal Adviser, United States Department of State, 19 October 2010, ⟨cli.re/yqEPeQ⟩, visited 4 March 2021, p. 55-56.

[80]*See supra* n. 47.

[81]D. Krebs, 'Global dangers and national obligations: Extraterritorial protection obligations in the Basic Law: The BND judgment and the debate about a "supply chain law"', *VerfBlog* 4 July 2020, DOI: 10.17176/20200604-133500-0.

[82]*G10 Act* case, *supra* n. 5, para. 219.

her functioning within the local community? Why should the introduction of such a restriction be considered justified when it does not ensure the general safety of the society in which the individual functions? The answer to these questions lies in clarifying whether the use of bulk surveillance can be regarded as a necessary measure to achieve a recognised objective of a democratic state, that is, to ensure public security. The Bundesverfassungsgericht explained that the use of bulk data collection is indeed necessary – because only in this way is it possible to carry out analyses that may lead to identifying sources of potential threats to state security.[83] The Court stressed that there are no other less intrusive ways to achieve this goal; in particular, no narrower, more selective collection of data. This is one of the key arguments supporting the judgment, because it leads to the conclusion that, in principle, mass surveillance can be reconciled with the values of a democratic state governed by law, and the way in which it operates.[84] The Court reached this conclusion based on the way BND programmes are implemented, in which data is gathered with the use of selectors so that the amount of data collected can be progressively reduced at subsequent stages of automatic processing.[85] At the same time, however, the Court noted that the selection of search terms, as well as the collection, processing and use of data, must be subject to detailed legal regulation.[86] Therefore, it defined guidelines that the legislature should take into account so that the final shape of the new surveillance regulations would be in line with the Basic Law.

The Court also reiterated that general security objectives cannot be regarded as sufficient justification for interference in a strictly protected area of individual privacy.[87] As a result, it was the Court's view that legal safeguards applied in the area of foreign surveillance must include both the prohibition of selectors aimed at collecting sensitive information, and the obligation to remove this kind of information at the stage of manual analysis[88] if it has been collected accidentally.[89]

[83] *BND Act* case, *supra* n. 4, para. 144.

[84] *BND Act* case, *supra* n. 4, paras. 136 and 154.

[85] *BND Act* case, *supra* n. 4, para. 209.

[86] According to the arguments presented, this should include, in particular, regulations concerning the use of filter techniques, purposes of monitoring, the design of the monitoring process, a focused handling of search terms, the limits of traffic data storage, methods of data evaluation, the protection of confidentiality relationships and that of the core area of private life, as well as the specification of deletion obligations. *See BND Act* case, *supra* n. 4, para. 169.

[87] *BND Act* case, *supra* n. 4, para. 200; *see also* BVerfG 3 March 2004, 1 BvR 2378/98, para. 120: '[T]he development of personality in the core area of private life includes the possibility of expressing internal processes such as sensations and feelings as well as reflections, views and experiences of a highly personal nature, without fear that government agencies will monitor it'.

[88] *BND Act* case, *supra* n. 4, para. 205.

[89] *BND Act* case, *supra* n. 4, para. 207.

Data sharing regime and international intelligence cooperation

In its earlier case law, the Bundesverfassungsgericht not only approved the admissibility of automatic data transfer abroad, it also stressed the importance of maintaining the 'principle of reciprocity' for the success of international intelligence cooperation.[90] However, in the *BND Act* judgment, the Court considered the current legal regime for cross-border data transfers to be incompatible with the Basic Law.[91] The Court reiterated its previous position in this respect, as presented in the *BKA Act* case.[92] First of all, it stressed that one condition governing the transfer of data is to ensure that it is not used in a way that is incompatible with the purpose of its collection, and that equivalent legal remedies are available to individuals under surveillance in the receiving countries. Significantly, as the Court pointed out, the transfer of data cannot be based on a discretionary political decision and must be based on verifiable, up-to-date and reliable information, so that it can be subjected to independent scrutiny.[93]

Due to constitutional provisions, the Court ruled out the possibility of transferring data to recipients who could use it in a way that violated human dignity (including for the purposes of political struggle or inhuman or inhumane treatment).[94] Although the wording of the *BND Act* judgment does not explicitly refer to the BND's cooperation with the NSA, this context cannot be ignored – especially given the importance of this cooperation as a premise for the introduction of the provisions under constitutional review. This cooperation consisted not only of transferring data to the NSA, but also of using selectors defined by the US partner. In this regard, the question was raised as to whether the use of BND powers to collect data that had been received by the foreign service influenced in any way the achievement of German intelligence's statutory objectives. An indirect response to this issue can be found in the *BND Act* requirement that the future transfer of data to a foreign partner should be permissible only if it does not jeopardise guarantees relating to respect for the fundamental right to personal data protection.[95] Although the Court did not refer to the concept of adequacy of safeguards, as enshrined in EU data protection law,[96] it follows from the arguments presented

[90]BVerfG 13 October 2016, 2 BvE 2/15, para. 165.

[91]*BND Act* case, *supra* n. 4, para. 320.

[92]*BKA Act* case discussed in more detail in: R.A. Miller, 'A Pantomime of Privacy: Terrorism and Investigative Powers in German Constitutional Law', 58 *Boston College Law Review* (2017) p. 1545.

[93]*BND Act* case, *supra* n. 4, para. 241; also *BKA Act* case, *supra* n. 6, para. 339.

[94]*BND Act* case, *supra* n. 4, para. 237.

[95]*BND Act* case, *supra* n. 4, para. 236.

[96]Adequacy of protection is a fundamental requirement for the admissibility of cross-border data transfers outside the EEA area, as applied in the EU data protection law. US legislation's failure to meet the adequacy criterion was one of the reasons for the European Court of Justice voiding the Safe Harbour and Privacy Shield programmes. An in-depth analysis of the adequacy criterion goes

that it is not possible to carry out data transfers to a third country if its legal model does not provide for systemic protection of personal data.[97]

While the considerations presented in the *BND Act* judgment almost reproduce the arguments presented in the *BKA Act* case, it should be borne in mind that in its most recent judgment the Court referred to the activities of intelligence services – not only of law enforcement agencies. Moreover, in the *BKA Act* case, only transfers of data to security and intelligence agencies in third countries (outside the EU/EEA) were examined, whereas the *BND Act* judgment does not contain such a limitation. As a result, although the constitutional standard defined in both cases is very similar, it was applied to a wider extent in the *BND Act* judgment.

The impact of the judgment in the *BND Act* case on European law

From the perspective of seeking a common European consensus on the limits of permissible foreign surveillance, the judgment in the *BND Act* case is important for several key reasons.

Firstly, the Bundesverfassungsgericht was the first EU constitutional court to make a direct statement on the need to apply fundamental rights – the common *acquis* of the European legal model – to all activities of public authorities, including those carried out abroad. Although this judgment does not in any way bind other constitutional courts, the position of the Karlsruhe judges will certainly be examined in detail in the capitals of other European countries. The way in which fundamental rights are defined and protected in these countries is almost identical, which obviously results from the fact that their national legal systems have been under the influence of European Court of Human Rights case law for more than sixty years, as well as from integration processes within the EU, which have taken place for almost as long. Hence, although this argument can be described as speculative, it seems unlikely that a similar analysis of the extraterritorial effect of fundamental rights by the constitutional court of another EU member state would lead to significantly different conclusions.

beyond the scope of this article, but it should be noted that the correctness of this concept has been discussed for years. In the author's view, the BVerfG's departure from the adequacy requirement is reasonable, as it does not attempt to impose the EU model of data protection legislation on non-EEA countries.

[97]This is not without significance when it comes to assessing the legal model of the US – especially to the extent that the norms of US federal law provide for the supremacy of national security goals over the rights of individuals.

https://doi.org/10.1017/S1574019621000055 Published online by Cambridge University Press

Secondly, the German surveillance regulations are – also when compared to other EU member states – a rare example of the national legislature deciding to clarify the competence of intelligence services for foreign electronic surveillance programmes. In the vast majority of European countries such provisions do not exist, and foreign intelligence agencies' power to conduct surveillance programmes is derived from blanket statutory powers.[98] Thus, the Bundesverfassungsgericht judgment not only supports the concept of the extraterritorial effect of fundamental rights, but it also contains an important analysis that helps determine a feasible standard of legal safeguards that should be implemented. In this context, 'feasible' refers to a type of control that, without paralysing the operation of intelligence services, puts the area of foreign-foreign surveillance under a supervision and control regime applicable to other surveillance measures. From the perspective of those EU countries where there are no provisions similar to those assessed by the Bundesverfassungsgericht, this judgment may therefore provide important guidance on how to shape future national regulations to take due account of the requirements of proportionality and necessity.

The *BND Act* judgment may also be helpful in developing a common standard for the cross-border exchange of information within the framework of criminal and national security cooperation. These two areas of supranational cooperation intermingle.[99] Information obtained as part of intelligence activities is used in the area of combating serious crime. Cooperation in criminal matters is also subject to EU regulations, but only to the extent that it does not cover the area of national security.[100] At the same time, however, the very decision to transfer data constitutes an interference with fundamental rights.[101] Therefore, the Bundesverfassungsgericht judgment may be helpful in defining a common minimum standard of safeguards to be applied as part of agreements – including those concluded under Article 73 of the TFEU – so that both the scope of the data transferred and the way in which it is used are similarly defined and

[98]An example is the Polish Act on the Internal Security Agency and the Foreign Intelligence Agency, which defines 'conducting electronic intelligence' as one of the tasks of the Foreign Intelligence Agency (Art. 6(1)(8)). The legislature did not impose any limitations on the scope of performing this task, except for the indication that, as a rule, the activities of the Agency should be carried out outside the country (Art. 6(3)).

[99]For example, in EU law the fight against terrorism is included in both criminal and national security cooperation activities. As a result, the Union has the power to introduce provisions harmonising national laws in the field of combating terrorism (e.g. Directive 2017/541). At the same time, however, EU institutions, including the European Court of Justice, have placed the fight against terrorism among the tasks undertaken by states in the area of national security – i.e. activities excluded from EU law (*see* e.g. ECJ 4 June 2013, Case C-300/11, *ZZ* v *Secretary of State for the Home Department*).

[100]Such a limitation follows directly from Art. 73 of the TFEU.

[101]*BND Act* case, *supra* n. 4, para. 212.

https://doi.org/10.1017/S1574019621000055 Published online by Cambridge University Press

interpreted, regardless of whether the transfer of data takes place in the sphere of the fight against serious crime or in pursuit of national security objectives.

Unfortunately, the Bundesverfassungsgericht avoided taking a stance on possible discrimination against EU citizens resulting from the establishment of separate laws governing the use of surveillance. In the opinion of the Karlsruhe judges, answering this question will be possible if – first and foremost – the scope of the national security clause provided for in Article 4(2) of the TEU is clarified under EU law. If the BND's activities related to foreign surveillance fall, even partially, within the scope of EU law, then the assessment of possible discrimination against EU citizens must take into account the provisions of the Charter of Fundamental Rights and the case law of the Luxembourg Court.

At the time of the Bundesverfassungsgericht judgment,[102] the European Court of Justice was examining questions referred for a preliminary ruling concerning the issue of whether and to what extent member states may apply a general data retention obligation in order to collect metadata derived from electronic communications and transmit them to national intelligence services. The Bundesverfassungsgericht considered that the answer to these questions was crucial in clarifying the scope of application of EU law to foreign surveillance. In judgments delivered on 6 October 2020, the Court of Justice, following the opinion of the Advocate General,[103] held that member states cannot invoke the exemption relating to the pursuit of national security objectives when they impose, by means of national law, an obligation to carry out specific tasks (such as a general data retention obligation) on commercial entities.[104] The judgment in the *Privacy International* case, although it confirms the incompatibility of the general data retention obligation with EU law, has not contributed to a significant clarification of the national security clause's limits. In particular, the ruling does not indicate clearly whether the activities of countries implementing extensive surveillance programmes that enable the interception of bulk quantities of data from other member states actually comply with EU law. Inasmuch as the Bundesverfassungsgericht did not decide to formulate its own preliminary questions in this area,[105] this problem should not be expected to be resolved in the near future.

[102]Reference for a preliminary ruling in cases: C-623/17, *Privacy International* v *Secretary of State for Foreign and Commonwealth Affairs and Others*, ⟨cli.re/yqR9PM⟩ and C-511/18, *La Quadrature du Net and Others* v *Premier ministre and Others*, ⟨cli.re/1kbjjz⟩, both visited 4 March 2021.

[103]Opinion of AG Manuel Campos Sánchez-Bordona in joined cases C-511/18 and C-512/18, *La Quadrature du Net and Others* v *Premier ministre and Others*, para. 85

[104]ECJ 6 October 2020, Joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* v *Premier ministre and Others*, paras. 103-104.

[105]The Court found that, since the regulations under review did not comply with constitutional provisions, the question of their compliance with EU law remained irrelevant for the resolution of the case. *See BND Act* case, *supra* n. 4, para. 112.

Conclusions

The judgment in the *BND Act* case is in line with ongoing discussion on the need to control electronic intelligence activities in democratic countries. The construction of the post-war human rights system was based on a supranational consensus that fundamental rights are universal, inalienable, and inviolable. Modern democracies, whose common feature is respect for human dignity, should not apply double standards depending on the geographical location of the person under surveillance.

The need to follow the same basic principles for regulating foreign surveillance as those governing various forms of national surveillance is not only based on moral concerns, but also practical ones. Assuming that cooperation between intelligence services is desirable and increases the effectiveness of their actions, it is also necessary to adopt a legal framework which will not be an obstacle to the transfer of data obtained from surveillance. The introduction of different rules for domestic and foreign surveillance clearly creates such a barrier and – as shown by information revealed on cooperation between the NSA and European intelligence services – a real possibility of abuse. Any attempt to refer territorially-defined surveillance procedures to transnational digital services would lead to opaqueness and be difficult to monitor, and therefore less effective and more prone to error.

However, recognition of the extraterritorial application of fundamental rights in the area of foreign surveillance does not necessarily lead to the introduction of the same legal restrictions as those applicable to domestic surveillance. Compliance with the principle of proportionality requires weighing the interests at stake and demonstrating the need for the interference in question. Even in the *BND Act* judgment, the Bundesverfassungsgericht pointed out that foreign intelligence activities involving the collection of electronic data are characterised by a lower degree of interference than identical measures that are applied domestically.[106] This is due to the simple fact that the individual is not subject to state control. In a similar way, it is possible to consider that some legal safeguards – such as the information obligation towards the individuals concerned – do not apply to foreign intelligence activities. This, however, does not affect the conclusion that foreign surveillance programmes should be carried out in accordance with the rule of law and not lead to a violation of human dignity. Therefore, programmes of this type, especially if they are based on the bulk collection of data, should be implemented with the use of externally-evaluated, detailed procedures that minimise the scope of the data collected and processed.

[106] *BND Act* case, *supra* n. 4, para. 149.

The impact of the *BND Act* judgment on the discussion concerning the scope of admissible surveillance undertaken in European countries seems particularly interesting.[107] The constantly evolving process of digitisation means that more and more activities of both individuals and public authorities are being carried out by means of IT systems. The EU's current strategy and priority is to transform members' economies to ones based on knowledge and data. However, the success of the project to build a single digital market requires member states to refrain from using measures that could constitute an obstacle to its operation. In the digital world, such a measure, in addition to the classic economic mechanisms of state influence on the economy, may also lead to the use of unlimited surveillance. The bulk interception of communications from other member states is not necessary to protect national security. Similarly, cooperation with the intelligence services of third countries in order to eavesdrop on European neighbours does not strengthen mutual trust among EU countries. As a result, the question of the scope of admissible electronic surveillance aimed at other member states is, in fact, a question about the future of European integration, i.e. whether it will remain a mechanism of limited economic cooperation, or if it will develop into a supranational union of values.

[107]This issue has been discussed for years now. Recently it has been addressed in resolution 2045 (2015) of the Parliamentary Assembly of the CoE on mass surveillance, which proposed to start work on the development of the so-called 'Intelligence Codex'. For more, *see* E. Watt, 'The right to privacy and the future of mass surveillance', 21 *The International Journal of Human Rights* (2017) p. 773.

https://doi.org/10.1017/S1574019621000055 Published online by Cambridge University Press