German Law Journal (2022), **23**, pp. 173–185
doi:10.1017/glj.2022.12

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Consequences of the German Constitutional Court's Ruling on Germany's Foreign Intelligence Service: The Importance of Human Rights in the Cooperation of Intelligence Services

Katrin Kappler

Max Planck Institute for the Study of Crime, Security and Law, Freiburg, Germany
Corresponding Author Email: k.kappler@csl.mpg.de

(Received 02 September 2020; accepted 18 January 2021)

Abstract
In 2020, Germany's Federal Constitutional Court made a groundbreaking decision on foreign surveillance by the Federal Intelligence Service, the Bundesnachrichtendienst (BND). The Court's first central finding was that the protection of fundamental rights is not limited to German territory. In addition, the ruling declared unconstitutional the regulations governing the transfer of information to foreign intelligence services. The ruling will therefore also have consequences for the cooperation of intelligence services, making it relevant abroad as well. In the ruling, the Court focused primarily on the role of human rights and ruled that the BND must check whether its cooperation partners respect human rights. The German parliament was given the task of implementing the Court's demands. The law adopted in response to the Court's demands came into force at the start of 2022. This article analyzes the ruling and the new law, and addresses the question what concrete requirements must be placed on the BND's cooperation with foreign intelligence services.

Keywords: Intelligence Law; Human Rights; Surveillance Law; Intelligence Cooperation

A. Introduction

The Snowden revelations provoked broad discussion in Germany, including an official Committee of Inquiry ("NSA Untersuchungsausschuss"). Among other things, the Committee's report concluded that the Federal Intelligence Service, the Bundesnachrichtendienst (BND) had no legal basis for authorizing foreign intelligence.[1] The German parliament reacted by reforming the BNDG (Gesetz über den Bundesnachrichtendienst) (BND Act) in 2016. At that time, the legislature maintained that the BND was not bound by the Basic Law (Grundgesetz) abroad. On May 19, 2020, the First Senate of the Federal Constitutional Court ruled that these reforms were largely unconstitutional and held that the Basic Law—especially Article 10, privacy of telecommunications, and Article 5, press freedom—binds the BND, even where foreigners in a foreign country are involved.[2] This judgment made clear that because Germany does not act alone, legal orders

Katrin Kappler is a Postdoc in the Department of Public Law at the Max Planck Institute for the Study of Crime, Security and Law.

[1]Beschlussempfehlung [Recommendation], Deutscher Bundestag: Drucksache [BT] 18/12850, 1613-1614.

[2]Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], 1 BvR 2835/17, (May 19, 2020), http://www.bverfg.de/e/rs20200519_1bvr283517en.html. *See* Benedikt Reinke, *Rights Reaching Beyond Borders: A Discussion of the BND-Judgment,*

beyond national law are relevant; that is, integration into the international community of states entails obligations. In the judgment, the Court drew on international law to make clear that fundamental rights cannot stop at Germany's national borders because this would not correspond to integration into international state power. In addition, the judgment demonstrates that international law in the form of human rights is relevant when a German intelligence service cooperates with foreign intelligence services. Specifically, the Court ruled that in cases where data is transferred to foreign entities, the legislature must require recipients to use the data in accordance with the rule of law.[3] An important question that arises from the BND judgment is what influence the judgment will have on foreign intelligence cooperation. For this reason, the judgment should also be considered beyond Germany's national borders. This article takes a critical look at the ruling and how it will be implemented under the fundamentally revised BNDG, which will come into force at the beginning of 2022.

B. Legal Basis and Key Aspects of the Judgment

I. Legal Framework of Surveillance Law in Germany

The BND is one of Germany's three federal intelligence services, along with the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz), and the Military Counter-Intelligence Service (Militärischer Abschirmdienst), and is responsible for civil and military foreign intelligence. The BND operates on the basis of the BNDG, a law passed in 1990. This law also allowed surveillance of foreigners abroad to obtain information. The legislature assumed that this would not violate any fundamental rights. Therefore, the legislature also refrained from designating the fundamental rights as restricted in the law (Zitiergebot - citation requirement) and set no guardrails on the surveillance of entirely foreign communications. For cooperation with foreign intelligence services, the details of the cooperation must be laid out in a letter of intent. Amongst other things, the law allows collected data to be used only where such use accords with fundamental principles of the rule of law. These principles include in particular the principles of democracy, separation of powers, protection of human dignity and other human rights, and judicial protection. It was therefore argued that cooperation with totalitarian regimes is not permissible. The government's official justification for the law shows that transmission should not be allowed to occur if elementary requirements of human protection are undermined[4]. It was also pointed out in the literature that transmission cannot take place if torture is imminent. A data transfer to member states of the European Union has so far not been considered inadmissible. This was rightly justified with the EU Charter of Fundamental Rights. As a rule, commitment to these rights must be sufficient to demonstrate compliance with human rights. However, the situation is different if there is sufficient doubt that these human rights are actually being observed.

II. Key Aspects of the Judgment: Basic Rights for Foreigners and Human Rights as Limit for Data Transfer

1. Basic Rights Also Apply to Foreigners Abroad

The main and groundbreaking[5] holding of the judgment is that the BND is also bound by the Basic Law abroad.[6] This is the first time that the Court has affirmed the application of

Dated 19 May 2020, 1 BvR 2835/17, VERFASSUNGSBLOG (May 30, 2020), https://verfassungsblog.de/rights-reaching-beyond-borders.

[3]1 BvR 2835/17 at para. 231.

[4]Gesetzentwurf [Bill], Deutscher Bundestag: Drucksache [BT] 18/9041, 34.

[5]Russel A. Miller, *The German Constitutional Court Nixes Foreign Surveillance*, LAWFARE (May 27, 2020), https://www.lawfareblog.com/german-constitutional-court-nixes-foreign-surveillance.

[6]1 BvR 2835/17 at para. 87-110. This problem has already been extensively discussed in the literature. *E.g.* Klaus Ferdinand Gärditz, *Die Reform des Nachrichtendienstrechts des Bundes: Ausland-Ausland-Fernmeldeaufklärung des*

German fundamental rights to situations outside German territory.[7] The Court explained that the Basic Law binds every form of German state power, even if it acts in a foreign context, because Article 1(3) states that the basic rights shall bind the legislature, the executive, and the judiciary as directly applicable law. No limitation could be inferred from the wording.[8] Moreover, the Court argued that this interpretation is consistent with Germany's integration into the world's community of states, including the alignment of human rights.[9] It is already striking how intensively the Federal Constitutional Court incorporates international law by considering the legal situation under the European Convention on Human Rights (ECHR). This has the potential to bring about a rethinking beyond the individual case: Due to the manifold interrelationships between international and national law and international cooperation, the Basic Law must be interpreted and applied in accordance with international law.[10]

2. Human Rights as a Limit for Data Transfer to Foreign Intelligence Services

In addition, the judges addressed cooperation between the intelligence agencies and concluded that special requirements apply to the transmission of data to foreign agencies.[11] The Court insisted that the legislature demand constitutional protections on both sides of transfer,[12] holding that the same requirements that apply to the transmission of data to domestic offices apply also to the transmission of data to foreign agencies.[13] In particular, this means that the threshold of interference for data transmission must be specified. This is important because the data collection itself does not require a threshold of interference but is independent of the occasion.[14] The Court concluded that the knowledge gained regardless of the event can be made accessible for further processing only if a survey according to general rule of law requirements for transmission purposes would be justified.[15] Therefore, a sufficiently specific risk situation is necessary for the transmission.[16] In addition, the Court imposed further requirements for transmissions to foreign bodies—according to the judges, the rule of law needs to be verified by the BND.[17] This includes both the safeguarding of data protection guarantees and the safeguarding of human rights when using the information.[18] This requires sufficiently clear and specific legal standards that ensure this assurance of the BND.[19] The Court makes it clear that this does not mean that the same standards exist as in Germany. But from the judges' point of view, it is clear that human rights guarantees for the protection of personal data must be observed.[20] In addition, transmission is always ruled out if elementary principles of the rule of law are violated.[21] For clarification, the German Constitutional Court mandates compliance with the ECHR and other international human rights

Bundesnachrichtendienstes und Stärkung des Parlamentarischen Kontrollgremiums, 132 D. VBL. 525, 528 (2017); Jan Hecker, *Allgemeine Verfassungsfragen der Nachrichtendienste*, in HANDBUCH DES RECHTS DER NACHRICHTENDIENSTE, 221, 244–247 (Jan-Hendrik Dietrich, Sven R. Eiffler, & Josephine Asche eds., 2017); Sven Hölscheidt, *Das neue Recht des Bundesnachrichtendienstes*, 2 JUR. A. 148 (2017).

[7] Helmut Philipp Aust, *Auslandsaufklärung durch den Bundesnachrichtendienst*, 16 DÖV 715 (2020).

[8] 1 BvR 2835/17 at para. 88.

[9] *Id.* at para. 93-103.

[10] Aust, *supra* note 7, at 718.

[11] 1 BvR 2835/17 at para. 231.

[12] *Id.*

[13] *Id.* at para. 232.

[14] *Id.* at para. 218.

[15] *Id.*

[16] *Id.* at para. 222.

[17] *Id.* at para. 233.

[18] *Id.*

[19] *Id.*

[20] *Id.* at para. 236.

[21] *Id.* at para. 237.

treaties.[22] The judgment requires that the information not be used to persecute certain population groups, to suppress opponents, to kill or torture people in violation of international human rights law or international humanitarian law, or to detain people without a fair trial.[23] Addressing the extent of the assurance, the Court held that an individual examination is not always necessary. Rather, a general factual assessment of the situation in the recipient country is generally sufficient.[24] If the general assessment yields doubts, individual commitments must be obtained.[25]

C. Legal Requirements to Ensure Compliance with Human Rights

The German Constitutional Court also built on what had already been recognized in international law—intelligence agencies are bound by human rights, at least if the information transmitted concerns individuals[26] who cannot be attributed to a state.[27] Snowden's revelations have shown that this is no longer the exception.[28] Because there are many forms of intelligence cooperation and the question of respecting human rights can be raised only in individual cases,[29] it was also determined that a general statement of the extent to which a given intelligence service upholds human rights is not possible.[30] However, in its current legal practice, the German Constitutional Court demands exactly that—namely, a general assessment of whether human rights are respected in the recipient country.[31] What is missing, however, is an exact definition of the standards. Although human rights are mentioned as a point of reference, the verdict is very vague on this point. The Court even explicitly points out that the BND is supposed to form its own opinion on the international legal regulations to be observed. This is a major task in view of the fact that the BND, like the legislature before the ruling, was not even convinced that it was bound by fundamental rights abroad. The following section will therefore analyze which human rights must be respected.

I. Extraterritorial Scope of Human Rights Treaties

This inconsistency raises an already well-known question—whether human rights also apply extraterritorially.[32] The German Constitutional Court evidently presupposes its own idea in the BND judgment in question here, by not over-dealing with whether human rights also apply beyond national borders. Israel and the United States, for example, doubt whether universal human rights treaties can be applied extraterritorially.[33] However, it is also obvious that both

[22] *Id.* at para. 237.

[23] *Id.*

[24] *Id.* at para. 239.

[25] *Id.*

[26] *See* James Crawford, Brownlie's Principles of Public International Law 111 (2019) for further information on subjects of international law, especially in the field of international human rights.

[27] Stefanie Schmahl, *European Intelligence and Rule of law*, in Intelligence Law and Policies in Europe: A Handbook 291, 297 (Jan-Hendrik Dietrich & Satish Sule eds., 2019).

[28] *See* Stephen I. Vladeck, *Big Data Before and After Snowden*, 7 J. Nat'l Sec. L. & Pol'y 333 (2014).

[29] Helmut Philipp Aust, *Spionage im Zeitalter von Big Data—Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht*, 52 A. Vr. 375 (2014).

[30] Schmahl, *supra* note 27, at 295.

[31] 1 BvR 2835/17 at para. 239.

[32] Schmahl, *supra* note 27, at 298; Peter Margulies, *The NSA in a Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 Fordham L. Rev. 2137 (2014).

[33] U.N. Human Rights Committee (HRC), *Concluding Observations on the Fourth Periodic Report of the United States of America*, para. 4, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014); HRC, *Concluding Observations on the Fourth Periodic Report of Israel*, para. 4, U.N. Doc. CCPR/C/ISR/CO/4 (Nov. 21, 2014).

the International Court of Justice (ICJ)[34] and the UN Human Rights Committee[35] judge this question differently.[36] Employing the same reasoning as the German Constitutional Court, they endorse the view that anybody directly affected by a state party's action will be subject to state jurisdiction if the state has effective control.[37] This view is based on the assumption of the universality of human rights. The European Court of Human Rights (ECtHR) has been arguing similarly for some time. Following *Bankovic* in 2001, which held that the Convention States exercise jurisdiction only in their own territory,[38] the ECtHR in *Al-Skeini* has moved away from this view without fully abandoning the territorial concept of jurisdiction.[39] *Schmahl* argues convincingly that even though the concept of jurisdiction no longer fits new technologies, the exceptions in *Al-Skeini* apply nonetheless.[40] Because developments in digital technologies challenge traditional tests of effective control, the question naturally arises as to what effective control means in the context of government surveillance.[41] Particularly problematic is the collection of big data.[42] To the extent that surveillance activities involve the collection of big data, one cannot speak of effective control being exercised over all data.[43] In comparison, effective control can certainly be assumed in cases in which a comprehensive analysis of the data of a particular person is carried out and the data acquisition and evaluation are substantiated.[44]

II. Relevant Material Provisions

International law makes no direct statement about the admissibility of espionage,[45] which is why the principle "everything that is not prohibited is allowed" applies.[46] However, this does not mean that espionage in all forms is permissible.[47] Human rights in particular are a form of constraint on espionage. Besides the explicitly mentioned right to data protection, the definition of human rights relevant to the assessment is the key question.

[34]Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 108 (July 9).

[35]HRC, *General Comment No. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights [hereinafter ICCPR], on the Right to Life*, ¶ 63, U.N. Doc. CCPR/C/GC/36 (Oct. 30, 2018) ("In light of article 2, paragraph 1, of the Covenant, a State party has an obligation to respect and to ensure the rights under article 6 of all persons who are within its territory and all persons subject to its jurisdiction, that is, all persons over whose enjoyment of the right to life it exercises power or effective control. This includes persons located outside any territory effectively controlled by the State, whose right to life is nonetheless impacted by its military or other activities in a direct and reasonably foreseeable manner.").

[36]There are also extensive analyses in the literature, for example, Ralph 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 J. Int'l L. 639 (2013); Schmahl, *supra* note 27, 299–307; Nowak's CCPR Commentary: U.N. International Covenant on Civil and Political Rights (William A. Schabas ed., 2019); Margulies, *supra* note 32.

[37]HRC, *supra* note 35, at ¶ 63; Schmahl, *supra* note 27, at 301.

[38]Bankovic v. Belgium, App. No. 52207/99, para. 80 (Dec. 12, 2001). For a closer look, see Cedric Ryngaert, *Clarifying the Extraterritorial Application of the European Convention on Human Rights*, 28 Utrecht J. Int'l and Eur. L. 57, 58 (2012).

[39]Al-Skeini v. United Kingdom, App. No. 55721/07, para. 142 (July 7, 2011), https://hudoc.echr.coe.int/eng?i=001-105606; Barbara Miltner, *Revisiting Extraterritoriality After Al-Skeini: The ECHR and Its Lessons*, 33 Mich. J. Int'l L. 693 (2012); Ryngaert, *supra* note 38, 59.

[40]Schmahl, *supra* note 27, at 305.

[41]Margulies, *supra* note 32, at 2150.

[42]Aust, *supra* note 29, at 397.

[43]Aust, *supra* note 29, at 397.

[44]Aust, *supra* note 29, at 397–98. For further information on a virtual control test, *see* Margulies, *supra* note 32, 2150–51.

[45]Anne Peters, *Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part I*, EJIL: Talk! (Nov. 1, 2013), https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i.

[46]Aust, *supra* note 29, 378. *See* Craig Forcese, *Pragmatism and Principle: Intelligence Agencies and International Law*, 102 Va. L. Rev. Online 67, 68 (2016); *see also* Peters, *supra* note 45.

[47]Dieter Fleck, *Individual and State Responsibility for Intelligence Gathering*, 28 Mich. J. Int'l L. 687, 688 (2007).

1. Data Protection and Right to Privacy

The most germane human right named by the German Constitutional Court is the right to data protection.[48] There is no universal concept for data protection in public international law. In particular, there is no relevant international treaty and no developed state practice.[49] Nevertheless, the right to privacy is now understood to include cyberspace.[50] In connection with the international work of foreign intelligence services, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) is of particular importance and a universal standard.[51] For example, the UN Human Rights Council[52] and the UN Human Rights Committee[53] have emphasized that the right to privacy also applies to online communication. Thus, the systematic collection and storage of connection data as well as the interception of mobile conversations or online searches can interfere with the right to privacy.[54] However, not every intervention is a violation of Article 17.[55] This is shown by its wording, which speaks of *arbitrary* or *unlawful* interventions. Therefore, an intervention is justified if the national legal basis itself is also compatible with the ICCPR.[56] In this regard, the UN Human Rights Committee has, for example, criticized the legal foundations of the surveillance activities of the United States. In the 2014 state party report, the Committee suggested regulatory reforms requiring at least guarantees against data misuse.[57] In the report, the committee stated that it was also particularly important that individuals concerned have access to effective complaint mechanisms.[58] While the reforms urged by the Committee were formulated as recommendations, these reforms would best be considered necessary for the protection of rights under the ICCPR.[59] At the same time, the High Commissioner for Human Rights recognized that, provided surveillance takes place on grounds of national security or for the prevention of terrorism or another crime,[60] intelligence gathering is a legitimate governmental aim. Ultimately, this involves a tradeoff under the principle of proportionality.[61]

[48]Critical as to whether there is a right to data protection at all. Asaf Lubin, *"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, 18 CHI. J. INT'L L. 502, 510–18 (2018).

[49]Int'l Law Comm'n, Rep. on the Work of Its Fifty-Eighth Session, U.N. Doc. A/61/10, at para. 12. The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), Council of Europe, Jan. 28, 1981, sometimes applies in part, but not extraterritorially. *See* Aust, *supra* note 29, at 387–88.

[50]Schmahl, *supra* note 27, at 309–10; Anne Peters, *Surveillance Without Borders? The Unlawfulness of the NSA Panopticon, Part II*, EJIL: TALK! (Nov. 4, 2013), https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii.

[51]Aust, *supra* note 29, at 404.

[52]There is, for example, a Special Rapporteur on the Right to Privacy, who referred to G.A. Res. 2200 (XXI) A, ICCPR, Art. 17 (Dec. 16, 1966), and criticized the BNDG with the note that human rights do not apply only to people in Germany. Rep. of the Special Rapporteur on the Right to Privacy, U.N. Doc. A/71/368, ¶¶ 35–36 (Aug. 30, 2016).

[53]In connection with the NSA affair, the U.N. Human Rights Committee has also urged the United States to ensure that domestic and international surveillance activities are consistent with G.A. Res. 2200 (XXI) A, ICCPR, Art. 17 (Dec. 16, 1966). HRC, *Concluding Observations on the Fourth Periodic Report of the United States of America*, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014), https://digitallibrary.un.org/record/771176?ln=en.

[54]Schmahl, *supra* note 27, at 311.

[55]Peters, *supra* note 50.

[56]Aust, *supra* note 29, at 400–01. For further information, see Peters, *supra* note 45.

[57]HRC, *Concluding Observations on the Fourth Periodic Report of the United States of America*, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014), https://digitallibrary.un.org/record/771176?ln=en.

[58]*Id.*

[59]Aust, *supra* note 29, at 401–02.

[60]HRC, Rep. of the Office of the U.N. High Commissioner for Human Rights on the Right to Privacy in the Digital Age, ¶ 24, U.N. Doc. A/HRC/27/37 (June 30, 2014), https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

[61]Asaf Lubin, *The Liberty to Spy*, 61 HARV. INT'L L. J. 185, 223 (2020).

2. Universally Recognized Human Rights

The Court also prohibited data collection where elementary principles of the rule of law—for example, human dignity—are not followed.[62] From the judges' point of view, it is particularly important to prevent information from being used to (i) persecute particular population groups; (ii) suppress opponents; (iii) kill or torture people in violation of international human rights law or international humanitarian law; or (iv) detain people without due process.[63] Legislatures must ensure that the ECHR and other universal human rights treaties are complied with.[64] This is convincing because the upholding of internationally recognized human rights can be expected from every cooperation partner.[65] However, it is important to determine these universally recognized human rights. These include not only those human rights that are *jus cogens* but also the rights set out in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), and the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICRMW). This already follows from the United Nations' Millennium Declaration, in which 189 UN member states defined numerous binding goals and specified the concept of "internationally recognized human rights."[66] What is common to these contracts is that they have a high level of ratification—or, in the case of the UDHR, enjoy a high level of acceptance—and that they contain a large number of regulations under international law.[67] Accordingly, they serve as a good reference point in the field of intelligence services. By contrast, it is not convincing to attach such a high value to the ECHR because it is only a regional treaty that cannot claim universality.[68] This does not mean that the ECHR is superfluous in these cases, as the BND is bound by it.[69] However, this instrument does not apply to all intelligence agencies; it does not apply to U.S. intelligence agencies, for example.[70] That is why it is important to refer to *universal* human rights and, if necessary, to contextualize them with regional human rights treaties. This means that the intelligence agencies are bound by all the rights guaranteed in these universal human rights treaties and the BND must ensure that the information that is to be transmitted is not used for purposes that conflict with these rights. Besides the right to privacy, the prohibition of torture,[71] the right to life,[72] and the prohibition of discrimination[73] are particularly significant.[74]

---

[62]BVerfG, 1 BvR 2835/17, para. 237, (May 19, 2020), http://www.bverfg.de/e/rs20200519_1bvr283517en.html.

[63]*Id.*

[64]*Id.*

[65]Martin Kment, Grenzüberschreitendes Verwaltungshandeln: Transnationale Elemente deutschen Verwaltungsrechts 709 (Jus Publicum 194, 2010).

[66]G.A. Res. 55/2, Millennium Declaration (Sept. 8, 2000).

[67]Katrin Kappler,1 Die Verfolgungen wegen der sexuellen Orientierung und der Geschlechtsidentität als Verbrechen gegen die Menschlichkeit 108 (2019).

[68]*Id.*

[69]Jochen von Bernstorff & Josephine Asche, *Nachrichtendienste und Menschenrechte*, in Handbuch des Rechts der Nachrichtendienste, *supra* note 6, at 79, 81.

[70]*But e.g.,* both Israel and the United States have ratified the ICCPR.

[71]ICCPR Art. 7, para. 1, states, "No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. In particular, no one shall be subjected without his free consent to medical or scientific experimentation." This right is not only non-derogable but also ensured without any restriction whatsoever. *See* Schabas, *supra* note 36.

[72]ICCPR Art. 6(1) states, "Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life." *See* Schmahl, *supra* note 27, at 325–26; Schabas, *supra* note 36.

[73]The principle of equality runs like a thread throughout the ICCPR, for example, Arts. 2 and 3. ICCPR Art. 26 does not duplicate these guarantees but establishes an autonomous right. CCPR General Comment No. 18: Non-discrimination (Nov. 10, 1989), https://www.refworld.org/docid/453883fa8.html. It states that all persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

[74]Schmahl, *supra* note 27, at 315–26.

Of course, these rights do not all apply without restriction, but what is clear is that utmost consideration must be given to the principle of proportionality.[75] It is not clear why the set of human rights by which intelligence services are bound should be limited to basic human rights. It has been pointed out that the intelligence services are bound by human rights; if they do not fulfill their obligation to uphold human rights, they violate international law. If the aim is to prevent the circumvention of standards, this obligation must apply to all human rights without distinction. In addition, it must be recognized that it must be a *violation* of human rights and not only an infringement. References to fundamental human rights are therefore misleading. The new Section 30 of the revised BNDG—which came into force in January 2022—establishes a ban on transmission in cases of significant human rights violations or violations of elementary principles of the rule of law. The new Section 30 does not, however, limit the set of relevant human rights to fundamental human rights. The provision's limitation of the set of relevant human rights violations to those that are significant in nature is in line with the Federal Constitutional Court's ruling, as the Court also makes clear through its exemplary enumeration of killing and torture that significant human rights violations shall be prevented.

III. Scope of the Assurance

Another question raised by the BND judgment is the extent to which the BND must ensure compliance with the rule of law. Foreign agencies are not subject to German law,[76] and the BND has no control rights.[77] Therefore the question may remain theoretical. In addition, because intelligence activity is mostly secret, the information cannot easily be released.[78] In particular, the German Constitutional Court clarified that relying solely on compliance with the principles of the rule of law is not sufficient.[79] This means that even a formulaic declaration of compliance is not sufficient. Rather, the correctness and seriousness of such a declaration *must* be checked by the BND. If there are doubts about compliance with the rule of law, data transmission must not be allowed to occur.[80] This means that information transfers must not be allowed to occur if the receiving state has a questionable human rights record.[81] Moreover, intelligence cooperation must be guided by clear statutory authorization that ensures human rights are respected.[82] Though the answer will ultimately depend on the specific legal basis, these implications of the BND judgment raises the question of whether extensive data transfer to important cooperation partners is fundamentally compatible with the judgment. The examples of the United States, the United Kingdom, and Israel show that there can at least be doubts about respect for human rights. According to the new Section 30 BNDG, a data transfer must be stopped if it is *recognizable* to the Federal Intelligence Service that interests worthy of protection, which also includes elementary human rights, are not sufficiently protected in the recipient state. Here, the legislatures reverses the requirements set by the Court by not obliging the BND to *ensure* that human rights are respected but rather establishing that the violation must be recognizable to the BND. To this extent, the legislature does not comply with the requirements set by the Court.

[75]Schabas, *supra* note 36.

[76]Kment, *supra* note 65, at 705–06.

[77]Christoph Gusy, *Nachrichtendienste in der sicherheitsbehördlichen Kooperation*, in HANDBUCH DES RECHTS DER NACHRICHTENDIENSTE, *supra* note 6, at 349, 392.

[78]*Id.*

[79]1 BvR 2835/17, para. 239.

[80]Gusy, *supra* note 77, at 393.

[81]Miller, *supra* note 5.

[82]*Id.*

D. No More Information Transfer to Foreign Intelligence Services?

The way intelligence agencies operate has changed dramatically due to globalization.[83] No individual state can do the job alone.[84] Therefore, cooperation between intelligence agencies is urgently required.[85] This is also stated in the report of the *NSA Committee of Inquiry*, which states that the BND is dependent on cooperation with foreign intelligence services. The BND judgment brings into question whether this cooperation remains possible, even taking the low requirements of the current design as a benchmark. Whether a state respects human rights in relation to intelligence-related work can be determined from the state reports of international bodies, especially those of the UN Human Rights Committee. This issue will be the focus of the following analysis.

I. Intelligence Services in the United States

1. Legal Framework

The U.S. also has different intelligence services for different tasks. The Federal Bureau of Investigation (FBI) is responsible for domestic counter-terrorism, police investigations, prosecution of organized economic and violent crime, and counter-espionage. The Central Intelligence Agency (CIA) is the American foreign intelligence service. The National Security Agency (NSA) is also responsible for foreign countries, but it concentrates on signals intelligence. Although after the Snowden revelations the U.S. and especially the NSA were criticized by Germany in particular, it quickly became clear that the legal foundations of the U.S. and Germany did not differ very much with regard to surveillance abroad. At the core of the U.S. regulatory framework is the Foreign Intelligence Surveillance Act (FISA). The aim of this law is to set limits on surveillance abroad. In contrast, domestic surveillance is primarily regulated by the USA PATRIOT Act. As in Germany, different standards apply to domestic surveillance than to surveillance abroad. Under Section 702 of FISA, foreign entities and individuals can be targeted. According to this legal basis, private interests are respected only in the case of U.S. citizens—not in the case of foreigners.[86] According to dominant opinion, the U.S. Constitution operates in the same way: There are only limited possibilities for extraterritorial effect of the Constitution with regard to foreigners. This means especially that intelligence operations abroad against non-U.S. citizens are not affected by constitutional guarantees.[87] Due to the Snowden revelations, the Obama administration passed Presidential Policy Directive 28 (PPD-28).[88] which was not repealed by Trump. This Directive sets limits on mass surveillance and the same standards of protection for foreigners as for U.S. citizens[89] However, this does not establish subjective rights and does not have the force of law—none of this was codified in FISA itself.[90] Moreover, mass surveillance measures continue to be permissible for unlimited purposes so long as the data is stored for only a limited period of time.[91] Moreover, there is no mention of respect for human rights in the surveillance law of the U.S. With the new BND law, larger differences between the U.S. and German legal situations are emerging.

[83] Aust, *supra* note 29, at 376–77. Especially concerning big data. Kenneth Cukier & Viktor Mayer-Schoenberger, *The Rise of Big Data: How It's Changing the Way We Think About the World*, 92 Foreign Affs. 28 (2013).

[84] Gusy, *supra* note 77, at 394. In some cases, however, it is also pointed out that it is a new phenomenon that individual countries are trying to capture the communication behavior of large parts of the world's population. *See* Aust, *supra* note 29, at 377.

[85] BVerfG, 1 BvR 2835/17, para. 231, (May 19, 2020), http://www.bverfg.de/e/rs20200519_1bvr283517en.html; Gusy, *supra* note 77.

[86] Alec Walen, *Fourth Amendment Rights for Nonresident Aliens*, *in* Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair, 282, 282 (Russell A. Miller ed., 2017).

[87] *See* Russel A. Miller, *A Rose by any Other Name? The Comparative Law of the NSA-Affair*, in Privacy and Power, *supra* note 86, at 91-93.

[88] *Id.* at 69.

[89] Directive on Signals Intelligence Activities (Presidential Policy Directive 28) (PPD-28), 1 Pub. Papers § 4 (Jan. 17, 2014).

[90] Alec Walen, *supra* note 86, at 288.

[91] Alec Walen, *supra* note 86, at 288.

2. Human Rights Record

In addition, there are also doubts about human rights compliance at the factual level. In 2014, the Committee against Torture criticized that the U.S. did not provide information on the practices of extraordinary rendition, enforced disappearance, or on the extent of abusive interrogation techniques, such as waterboarding, used by the CIA on suspected terrorists.[92] The Committee clarified that the ban on torture is absolutely guaranteed and that no justification is possible.[93] Additionally, the Committee referred to its second general comment, in which it states that even exceptional circumstances like terror or war are not grounds for justification.[94] Moreover, the UN Human Rights Committee in 2014 was troubled by the operations and practices of two U.S. agencies in particular—the FBI and the NSA. The Committee expressed concern about racial profiling by the FBI[95] and focused on NSA surveillance with unusual specificity.[96] The Committee criticized not only the data collection methods of the NSA, but also the fact that NSA oversight does not work well and that there are no effective enforcement mechanisms.[97] Even though these fears are not new, they are likely to raise doubts about the compatibility of the intelligence services' work with human rights. In view of the principles described by the German Constitutional Court in the BND judgment, it is clear that data transfer will no longer be permissible without additional scrutiny, as there are doubts regarding human rights compliance. For this reason, the BND will have to be assured in each individual case that the transfer of information will not lead to human rights violations.

II. Israel as Example of a State with Only Rudimentary Regulation of Intelligence Services

1. Legal Framework

Israel is meant to serve here as an example of a whole series of states—namely, States in which the work of intelligence services is only rudimentarily regulated by law and is overseen to only a limited extent by legislatures, courts, and other institutions.[98] These include, for example, States like China, Russia, and Iran. It is difficult to find up-to-date information on the work of intelligence agencies. The difficulty of monitoring the work of intelligence agencies, given the fact that such work remains mostly secret, is particularly evident in the case of Israel. This lack of transparency and the at least partial lack of a legal basis are problematic with regard to the rule of law.[99] That is not to say that there is no legal basis at all. With the General Security Law 2002, the Knesset created a legal basis for the General Security Service (GSS). This has brought at least some intelligence activities out of secrecy. However, it is also clear that sensitive issues such as torture have remained shrouded in secrecy.[100] In addition, this legal framework is only for domestic surveillance, not for foreign telecommunications intelligence.[101] There is still no legal basis in these

[92]U.N. Committee Against Torture (CAT), *Concluding Observations on the Combined Third to Fifth Periodic Reports of the United States of America*, ¶ 11, U.N. Doc. CAT/C/USA/CO/3-5 (Dec. 19, 2014), https://digitallibrary.un.org/record/790513/?ln=en.

[93]*Id.*

[94]CAT, *General Comment No. 2: Implementation of Article 2 by States Parties*, ¶ 5, U.N. Doc. CAT/C/GC/2 (Jan. 24, 2008), https://undocs.org/en/CAT/C/GC/2.

[95]HRC, *Concluding Observations on the Fourth Periodic Report of the United States of America*, ¶ 7, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014), https://digitallibrary.un.org/record/771176?ln=en.

[96]*Id.* at ¶ 22.

[97]*Id.*

[98]Stefan Heumann, *German Exceptionalism? The Debate About the German Foreign Intelligence Service (BND)*, in PRIVACY AND POWER, *supra* note 86, at 357.

[99]Schmahl, *supra* note 27, at 333.

[100]*See* Shlomo Shpiro, *Intelligence Services and Political Transformation in the Middle East*, 17 INT'L J. INTEL. & COUNTERINTEL. 575, 575–600 (2004).

[101]Lubin, *supra* note 48, at 514.

matters. This is a significant difference from states like Germany. This deficiency alone ought to mean that data transfers are no longer possible without an assurance in each individual case.

2. Human Rights Record

Furthermore, even with little information on human rights matters, there remain considerable concerns as to whether Israel's intelligence agencies are compliant with the German Constitutional Court's criteria. Both the Committee against Torture and the Human Rights Committee are concerned about the use of torture by security agencies.[102] Therefore, it can at least be seriously doubted whether human rights are respected. In view of the German Constitutional Court's criteria, it can be assumed that cooperation with Israeli intelligence services is no longer permissible without obtaining assurances in each individual case that the information will not be used to commit human rights violations.

III. British Intelligence Services as Example of a Non-EU European State

The United Kingdom shall function here as an example of a European state that is not any longer subject to the standards of the European Union.

1. Legal Framework

There are three principal intelligence services in the UK: the Security Service (MI5), the Secret Intelligence Service (MI6), and the Government Communications Headquarters (GCHQ). Because the UK, unlike most other states, has no written constitution, there is no constitutional basis for the intelligence services. Nevertheless, there are other legal foundations. The Security Service Act 1989 and the Intelligence Service Act 1994 set out the principles on which the intelligence services operate.[103] These acts are very similar in design, but leave room for flexibility in view of the different areas of activity.[104] According to the 1989 Act, MI5 is responsible for the protection of domestic national security from threats internal or external to the British Isles.[105] More relevant to the aims of this article is MI6, which is the counterpart of the German BND and focuses on foreign and defense interests. In addition, it must be considered that after Snowden's disclosures, the legal framework was fundamentally revised.[106] The Investigatory Powers Act 2016 brought intelligence-agency and law-enforcement powers for surveillance of communications and access to communications data together in one place and extended the power to cover additional new technologies, for example, bulk collection of data.[107] At the same time, a "double-lock" approval process was also introduced, under which both the Secretary of State for the Home Department and subsequently a Judicial Commissioner must authorize a warrant before it can be issued. The key players in this oversight arrangement are the Judicial Commissioners, a set of judicial officials that includes and is headed by the

[102]CAT, *Concluding Observations on the Fifth Periodic Report of Israel*, ¶ 30, U.N. Doc. CAT/C/ISR/CO/5 (June 3, 2016), https://www.refworld.org/type,CONCOBSERVATIONS,ISR,57a99c6a4,0.html; HRC, *Concluding Observations on the Fourth Periodic Report of Israel*, ¶ 15, U.N. Doc. CCPR/C/ISR/CO/4 (Nov. 21, 2014), https://undocs.org/CCPR/C/ISR/CO/4.

[103]There are other sources that cannot be discussed here; for more information see Simon McKay & Clive Walker, *Intelligence Law in the United Kingdom*, in Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 119, 121–122 (Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz, Kurt Graulich, Christoph Gusy, & Gunter Warg eds., 2019).

[104]*Id.* at 120.

[105]*Id.*

[106]Ian Leigh, *Intelligence Law and Oversight in the UK*, *in* Handbuch des Rechts der Nachrichtendienste, *supra* note 6, at 553, 555.

[107]*Id.*, 563–564; Simon McKay & Clive Walker, *Legal Regulation of Intelligence Services in the United Kingdom*, *in* Handbuch des Rechts der Nachrichtendienste, *supra* note 6, at 1855, 1929.

Investigatory Powers Commissioner.[108] It seems to be no coincidence that one of these Judicial Commissioners testified as an expert before the German Constitutional Court; the Court had the Judicial Commissioners in mind as a model for the new supervisory body in Germany. However, this process does not require checking whether cooperation partners respect human rights. Thus, the legal standards that UK intelligence agencies must comply with differ in a small way from the standards that the German Constitutional Court requires German law to establish in this area.

2. Human Rights Record

In theory, therefore, the UK is well prepared: There is a legal basis for action abroad, and its monitoring mechanisms are used as a model beyond the UK. However, this does not mean that the intelligence services consistently respect human rights. Even before the Snowden disclosures, it was clear that the British intelligence services[109] were involved in the torture and kidnapping of terrorism suspects after 9/11.[110] The Snowden revelations had a major impact on UK intelligence agencies as they too were revealed to be involved in mass surveillance.[111] In this context, the ECtHR delivered its judgment in Big Brother Watch and others v. the United Kingdom—a case which is not yet final, but pending before the Grand Chamber.[112] In that case, which arose in the aftermath of the Snowden revelations, the Court considered in detail the UK surveillance regime and held that certain aspects of it violated Articles 8—the right to respect for private and family life—and Article 10—freedom of expression— of the Convention.[113] Moreover, in this case, the court was asked for the first time to consider the issue of an intelligence-sharing regime's compliance with the Convention. The judges concluded that there were no significant shortcomings in the application and operation of the U.S.–UK intelligence sharing regime and therefore that there was no violation of Article 8 ECHR.[114] This, along with the other issues described thus far in this paragraph, would be reason enough to doubt whether information can still be transmitted to British intelligence services. But there is yet more cause for concern. Namely, there are some doubts as to whether the British intelligence community upholds all human rights. A report by the Committee against Torture emphasized torture allegations against the UK. Following the publication of the report, the UK did not fully investigate these allegations, nor did the UK hold the perpetrators accountable.[115] In this respect, however, it should be noted that the alleged acts of torture, assuming the allegations are true, took place a considerable time ago and that there is no evidence that this mistreatment is still going on. Therefore, the allegations are not on their own sufficiently indicative of the current level of protection of human rights by the UK. This is particularly true in view of the new reforms. Therefore, a general assessment by the BND should be sufficient. Only when concrete evidence of human rights violations re-appears will case-by-case assurances become necessary.

IV. Conclusion

As a result, it can be stated that cooperation with foreign intelligence services will be associated with higher thresholds in the future. Even if one takes the lower hurdles of the revised BNDG as a

[108]Lord Carlile, *Communications and Security After Brexit*, in Terrorism and State Surveillance of Communications 5, 13–14 (Simon Hale-Ross & David Lowe eds., 2019); McKay & Walker, *supra* note 107, at 1928.

[109]For further information on the major institutions, see McKay & Walker, *supra* note 107, at 1859.

[110]Intel. and Sec. Comm. of Parliament, Detainee Mistreatment and Rendition: Current Issues (HC 1114) (June 28, 2018), https://isc.independent.gov.uk/wp-content/uploads/2021/01/20180628-HC1114-Report-Detainee-Mistreatment-and-Rendition-Current-Issues.pdf.

[111]Leigh, *supra* note 106, at 554–58.

[112]For further information, see Aust, *supra* note 7, 720-721.

[113]Big Brother Watch v. United Kingdom, App. Nos. 58170/13, 62322/14 and 24960/15.

[114]*Id.*

[115]CAT, *Concluding Observations on the Sixth Periodic Report of the United Kingdom of Great Britain and Northern Ireland*, ¶ 34, U.N. Doc. CAT/C/GBR/CO/6 (June 7, 2019), https://undocs.org/en/CAT/C/GBR/CO/6.

standard, data transfers to countries with only rudimentary regulations governing intelligence services will probably no longer be permissible. Here, assurance must be obtained on a case-by-case basis, and such assurances must be substantial—not merely formal—in nature. In the case of countries that, like the U.S., have a sufficient legal basis but a human rights record that indicates that human rights are not always consistently respected, assurance must likewise be obtained on a case-by-case basis. The only remaining countries with whom German intelligence agencies could cooperate without case-by-case assurance are Germany's European partners. Cooperation with European partners should remain possible under the standard articulated by the German Constitutional Court, at least so long as European human rights standards are formally and factually observed in those countries.

E. Outlook

The judgment is convincing. The German Constitutional Court has instructed the legislature to legally constrain intelligence activities. The Court draws particular attention to human rights as a limit. The new law fulfills some of the requirements of the ruling but does not fully implement the scope of assurance defined by the Federal Constitutional Court. This article has shown the room for improvement. In addition, the judgment also has the potential to wake up the international community of states. International security law is characterized like no other area by the absence of law and by informal agreements. The judgment should be taken as an opportunity to change this. As a first step, states should declare that they are aware that intelligence services too are bound by human rights and that this obligation also applies to actions by intelligence services that involve foreigners abroad. In a second step, an intergovernmental solution can then be initiated for human rights standards in the collection, exploitation, and transfer of data, as well as for effective law enforcement. There is a risk that Germany will not be able to export all of its own standards because German intelligence services depend on cooperation with foreign intelligence services. Nevertheless, such an advance would be an opportunity to reduce the lack of transparency and establish at least some human rights standards in an area where, to date, none have existed at all.

Cite this article: Kappler K (2022). Consequences of the German Constitutional Court's Ruling on Germany's Foreign Intelligence Service: The Importance of Human Rights in the Cooperation of Intelligence Services. *German Law Journal* **23**, 173–185. https://doi.org/10.1017/glj.2022.12