Developments

Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden

By Christian Schaller[*]

Abstract

This Article examines the statutory and constitutional legal framework governing the bulk collection of communication data by the German Federal Intelligence Service (*Bundesnachrichtendienst*, BND). German intelligence law distinguishes between certain categories of communications depending on the nationality and location of the participants. The provisions on the surveillance of foreigners abroad are far more permissive than those applying to the monitoring of communications that involve German nationals or foreigners in Germany. This differentiation is the consequence of a narrow interpretation by the German legislator of the personal and territorial scope of the right to privacy enshrined in Article 10 of the Basic Law. While there is no doubt that German nationals enjoy protection under Article 10 wherever their privacy is affected by the actions of the German State, current intelligence legislation is based on the understanding that foreigners are entitled to such protection only while staying in Germany. It will be argued that such discrimination is difficult to reconcile with German constitutional law because Article 10 protects every natural person without regard to nationality and because the Article's applicability is not limited to the territory of the Federal Republic of Germany. This means that the BND is bound by Article 10 irrespective of whether its surveillance activities affect German nationals, foreigners in Germany, or foreigners abroad. Arguably, the level of protection in transnational constellations may be subject to certain modifications. But if basic rights protection is taken seriously, the existing fragmented legislation should be replaced by a uniform statutory regime for strategic surveillance of international communications that meets the minimum standards of Article 10 without bearing reference to a person's nationality or location.

[*] Dr. Christian Schaller, Deputy Head of Global Issues, German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik, SWP), Berlin. E-mail: christian.schaller@swp-berlin.org. The author would like to thank the participants of the Transatlantic Dialogue on Cyberespionage, Surveillance, and the Protection of Privacy in the Digital Age (hosted in June 2016 by the University of Glasgow School of Law, the Robert Strauss Center for International Security and Law at the University of Texas at Austin, and SWP).

A. Introduction

The disclosures by Edward Snowden about the mass surveillance programs of the U.S. National Security Agency (NSA) have caused considerable public irritation in Germany.[1] In March 2014, the Federal Parliament (*Deutscher Bundestag*) established a Committee of Inquiry to investigate the potential involvement of the BND in the activities of the "Five Eyes" States (USA, United Kingdom, Canada, Australia, and New Zealand) in Germany.[2] The findings by the Committee have corroborated speculations about a rather extensive surveillance cooperation between the BND and NSA.[3] A prominent example was Operation Eikonal (2003–2008), which served the collection and sharing of telephone and Internet data captured at the world's largest Internet exchange point, DE-CIX in Frankfurt am Main.[4] It was reported that the BND, within the framework of this operation, had also transferred personal data of German citizens to the NSA.[5] In July 2016, the Parliamentary Control Panel (*Parlamentarisches Kontrollgremium*), which is part of the regular intelligence oversight

[1] *See generally* Stefan Heumann, *German Exceptionalism? The Debate About the German Foreign Intelligence Service (BND)*, *in* PRIVACY AND POWER: A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA-AFFAIR 349, 352–56 (Russell A. Miller ed., 2016); Matthias Schulze, *Patterns of Surveillance Legitimization: The German Discourse on the NSA Scandal*, 13 SURVEILLANCE & SOC'Y 197 (2015) (describing and analyzing the reactions by the German Government, political parties, the media, and advocacy groups).

[2] Antrag auf Einsetzung eines Untersuchungsausschusses [Motion for the Establishment of a Committee of Inquiry], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/843 (Ger.). *See also* Antrag auf Ergänzung des Untersuchungsauftrages des 1. Untersuchungsausschusses–Hilfsweise: Einsetzung eines Untersuchungsausschusses [Motion for an Amendment of the Mandate of the 1st Committee of Inquiry–Alternatively: Establishment of a Committee of Inquiry], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/7565 (Ger.).

[3] Beschlussfassung und Bericht des 1. Untersuchungsausschusses nach Artikel 44 des Grundgesetzes [Report of the 1st Committee of Inquiry According to Article 44 of the Basic Law], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/12850 (Ger.) [hereinafter Report of the 1st Committee of Inquiry]. Non-official notes on public hearings are available at *Überwachung*, NETZPOLITIK.ORG, https://netzpolitik.org/category/ueberwachung/ (last visited July 15, 2018). Some documents are available at *Bundestag Inquiry into BND and NSA*, WIKILEAKS, https://wikileaks.org/bnd-nsa/sitzungen/ (last visited July 15, 2018). *See also* Maik Baumgärtner et al., *Spying Close to Home—German Intelligence Under Fire for NSA Cooperation*, SPIEGEL ONLINE (Apr. 24, 2015), http://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html; *Germany Restarts Joint Intelligence Surveillance with US*, DW DEUTSCHE WELLE (Jan. 9, 2016), http://www.dw.com/en/germany-restarts-joint-intelligence-surveillance-with-us/a-18968519.

[4] *See* Report of the 1st Committee of Inquiry, *supra* note 3, at 835–909, 1260–64, 1366–1508.

[5] Georg Mascolo, Hans Leyendecker & John Goetz, *Codewort Eikonal*, SÜDDEUTSCHE ZEITUNG, Oct. 4, 2014, at 6.

system in Germany,[6] made public that the BND had also spied on EU and NATO partners.[7] Two months later, a classified report was leaked in which the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) complained about several grave and systematic violations of constitutional and statutory law committed by the BND.[8] Such revelations have increasingly turned the "NSA affair" in the public debate into a "BND affair." Against this background, the *Bundestag* passed a major intelligence law reform in 2016 to enhance oversight and regulate the competences of the BND more clearly.[9] A core component of the reform was a set of provisions on the collection of signals intelligence[10] regarding foreigners abroad (*Ausland-Ausland-Fernmeldeaufklärung*).[11] Although such operations are an important element of the work of the BND, this complex had not previously been subject to statutory regulation. The new regime is extremely detailed; it even addresses the surveillance of EU institutions,

[6] The Parliamentary Control Panel exercises overall control over the activities of the BND. Its members must be members of the *Bundestag*. The general competences of the Panel are regulated in a separate law. *See* Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes [Kontrollgremiumgesetz] [PKGrG] [Act on the Parliamentary Control of Federal Intelligence Activities], July 29, 2009, BGBL. I at 2346, last amended by Gesetz [G], Jan. 5, 2017 BGBL. I at 17 (Ger.).

[7] Unterrichtung durch das Parlamentarische Kontrollgremium, Öffentliche Bewertung des Parlamentarischen Kontrollgremiums gemäß § 10 Absatz 2 und 3 des Kontrollgremiumgesetzes zur BND-eigenen Steuerung in der strategischen Fernmeldeaufklärung [Notification by the Parliamentary Control Panel, Public Evaluation by the Parliamentary Control Panel According to § 10(2) and (3) of the Control Panel Act on the Operation of Selectors by the BND in the Field of Strategic Signals Intelligence], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/9142 (Ger.) [hereinafter Notification by the Parliamentary Control Panel].

[8] *See* Andre Meister, *Secret Report: German Federal Intelligence Service BND Violates Laws and Constitution by the Dozen*, NETZPOLITIK.ORG (Sept. 2, 2016), https://netzpolitik.org/2016/secret-report-german-federal-intelligence-service-bnd-violates-laws-by-the-dozen/. The full source document is reproduced at Andre Meister, *Geheimer Prüfbericht: Der BND bricht dutzendfach Gesetz und Verfassung–allein in Bad Aibling (Updates)* (Sept. 1, 2016), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/#Sachstandsbericht.

[9] Gesetz zur weiteren Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes [Act on the Further Development of Parliamentary Control of the Federal Intelligence Services], Nov. 30, 2016, BGBL. I at 2746 (Ger.); Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes [Act on the Collection of Foreign-Foreign Communications Intelligence by the Federal Intelligence Service], Dec. 23, 2016, BGBL. I at 3346 (Ger.). *See generally* CHRISTIAN SCHALLER, DETAILLIERTE REGELN FÜR DIE AUSLANDSÜBERWACHUNG: AUCH NACH REFORM DES BND-GESETZES BLEIBT RECHTLICHER UND POLITISCHER KLÄRUNGSBEDARF [DETAILED RULES FOR FOREIGN SURVEILLANCE: EVEN AFTER THE REFORM OF THE BND ACT THERE IS STILL NEED FOR LEGAL AND POLITICAL CLARIFICATION] STIFTUNG WISSENSCHAFT UND POLITIK [SWP] SWP-Aktuell No. 66/2016 (2016), https://www.swp-berlin.org/fileadmin/contents/products/-aktuell/2016A66_slr.pdf (Ger.).

[10] In the intelligence community, the collection and exploitation of signals transmitted from communication systems is generally referred to as "communications intelligence" (COMINT), which is a subcomponent of the concept of signals intelligence (SIGINT).

[11] The new provisions on *Ausland-Ausland-Fernmeldeaufklärung* have been included as Sections 6 through 18 of the BND Act. *See* Gesetz über den Bundesnachrichtendienst [BND-Gesetz, BNDG] [Federal Intelligence Service Act] [BND Act], Dec. 20, 1990, BGBL. I at 2954, 2979, last amended by Gesetz [G], June 30, 2017 BGBL. I at 2097 (Ger.).

authorities of EU Member States, and EU citizens.[12] Another interesting feature are the provisions on international intelligence cooperation and the exchange of personal data with foreign intelligence services.[13]

Mass surveillance and bulk collection of communication data are highly problematic from the perspective of international human rights law.[14] For Germany, which frequently presents itself as a champion of the rule of law in international relations, the refinement of its own intelligence legislation and oversight system was therefore also a matter of international credibility. In 2013, Germany and Brazil started an initiative at the United Nations leading to the adoption of several General Assembly resolutions on "The Right to Privacy in the Digital Age."[15] In the first of these resolutions, the General Assembly emphasized that unlawful or arbitrary surveillance of communications violates the right to privacy and might "contradict the tenets of a democratic society."[16] Therefore, all States were called upon to review their procedures, practices, and legislation with a view to ensuring the full and effective implementation of their obligations under international human rights law.[17] The 2014 follow-up resolution made clear that surveillance of digital communications is admissible only on the basis of "publicly accessible, clear, precise, comprehensive, and non-discriminatory" legal norms.[18] In December 2016, the General Assembly once more reaffirmed these claims.[19] It should be safe to assume that the Federal Government and the *Bundestag* are particularly dedicated to a thorough implementation of the standards promoted in the resolutions. Nevertheless, the following analysis will show that the statutory norms governing the activities of the BND are still not entirely in compliance with these standards.

---

[12] BND Act §§ 6(3), 7(2), 9(2), (3), (5), 10(2), (3), 15(1)(lit. 1a).

[13] Cooperation with foreign intelligence services and other foreign public authorities (*ausländische öffentliche Stellen*), including the collection and automated transfer of personal data, within the framework of *Ausland-Ausland-Fernmeldeaufklärung* is regulated in Sections 13 through 15 of the BND Act. The maintenance of shared data sets in cooperation with foreign public authorities is subject to Sections 26 through 30 of the BND Act.

[14] *See*, *e.g.*, Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L.J. 81 (2015); Anne Peters, *Privacy,* Rechtsstaatlichkeit*, and the Legal Limits on Extraterritorial Surveillance*, *in* PRIVACY AND POWER: A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA-AFFAIR 145 (Russell A. Miller ed., 2016).

[15] G.A. Res. 68/167 (Dec. 18, 2013); G.A. Res. 69/166 (Dec. 18, 2014); G.A. Res. 71/199 (Dec. 19, 2016). See also the corresponding resolution adopted by the U.N. Human Rights Council, U.N. Doc. A/HRC/RES/28/16 (Mar. 26, 2015).

[16] G.A. Res. 68/167, pmbl. para. 8 (Dec. 18, 2013).

[17] *Id.* at para. 4(c).

[18] G.A. Res. 69/166, pmbl. para. 16 (Dec. 18, 2014).

[19] G.A. Res. 71/199, pmbl. paras. 20, 22; para. 5(c) (Dec. 19, 2016).

For the purpose of legal analysis, two types of intelligence-related surveillance may be distinguished: (1) targeted surveillance of individual communications, based on a certain degree of suspicion against a particular person or organization; and (2) untargeted, non-suspicion-based surveillance, which is often associated with catchwords like "mass surveillance" or "bulk collection."[20] The Venice Commission of the Council of Europe uses the notion "strategic surveillance" for the latter type to accentuate the process of filtering out relevant information from a bulk of data that has been collected without particular suspicion.[21]

Electronic communication signals may be collected in a variety of ways—in particular by tapping fiber optic cables that connect certain countries or regions of the world or by intercepting communication streams from satellites.[22] Internet exchange points, which serve as a platform for providers to interlink their networks, are also often used as a point of access to obtain large quantities of communication data.[23] To separate potentially relevant from irrelevant communications, intelligence services employ complex algorithms.[24] These systems operate with so-called "selectors," which are either technical identifiers (telephone numbers, e-mail and IP addresses, etc.) or concrete search terms.[25] Basically, two categories of communication data are to be distinguished—content data (the spoken word, the content of a text message or e-mail, photos, videos, etc.) and metadata, which relate to the circumstances of the communication process (technical identifiers of the infrastructure and devices used by the participants, time and duration of the communication, location of the participants, etc.).[26] Stewart Baker, former General Counsel of the NSA, once said in a discussion in New York that "[m]etadata absolutely tells you everything about somebody's life. . . . If you have enough metadata you don't really need

[20] *See, e.g.*, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU—MAPPING MEMBER STATES' LEGAL FRAMEWORKS 17 (2015) [hereinafter FRA, MAPPING MEMBER STATES' LEGAL FRAMEWORKS]. *See also* FRA, SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU, VOL. II: FIELD PERSPECTIVES AND LEGAL UPDATE 29 (2017) [hereinafter FRA, FIELD PERSPECTIVES AND LEGAL UPDATE].

[21] EUROPEAN COMM'N FOR DEMOCRACY THROUGH LAW (VENICE COMMISSION), STUDY NO. 719/2013, UPDATE OF THE 2007 REPORT ON THE DEMOCRATIC OVERSIGHT OF THE SECURITY SERVICES AND REPORT ON THE DEMOCRATIC OVERSIGHT OF SIGNALS INTELLIGENCE AGENCIES 11 (2015).

[22] *See, e.g.*, Zygmunt Bauman et al., *After Snowden: Rethinking the Impact of Surveillance*, 8 INT'L POL. SOCIOLOGY 121 (2014); BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT AND CONTROL YOUR WORLD (2015).

[23] Bauman, *supra* note 22, at 122.

[24] *Id*. *See also* Report of the 1st Committee of Inquiry, *supra* note 3, at 219–35.

[25] Report of the 1st Committee of Inquiry, *supra* note 3, at 783–86.

[26] *See* Bauman, *supra* note 22, at 123.

content."[27] Rapid advancements in the design of big data algorithms like XKeyscore have provided States with the capacity to process immense amounts of such data in almost no time.

It seems that States are generally reluctant to enact strategic surveillance laws because such laws might reveal to some extent how much leeway their intelligence services enjoy in this domain or under which restrictions they have to operate. The European Union Agency for Fundamental Rights (FRA) found out in 2015 that almost all Member States of the EU (with the exception of Cyprus and Portugal) have enacted laws on targeted surveillance, whereas only five countries (France, Germany, the Netherlands, Sweden, and the United Kingdom) have a more or less detailed legislation covering untargeted surveillance activities as well.[28] The Council of Europe Commissioner for Human Rights noted that in many Council of Europe Member States, untargeted bulk surveillance is "either not regulated by any publicly available law or regulated in such a nebulous way that the law provides few restraints and little clarity on these measures."[29]

The design of domestic intelligence law has received little attention so far in international academic forums.[30] Most of the articles and papers that deal with the legal aspects of the BND's work have been written in the German language, addressing primarily German scholars and practitioners.[31] But there is obviously a demand for international dialogue on

---

[27] Alan Rusbridger, *The Snowden Leaks and the Public*, THE NY REVIEW OF BOOKS (Nov. 21, 2013), http://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public/ (quoting Stewart Baker).

[28] FRA, MAPPING MEMBER STATES' LEGAL FRAMEWORKS, *supra* note 20, at 18–26. *See also* FRA, FIELD PERSPECTIVES AND LEGAL UPDATE, *supra* note 20, at 40–48.

[29] COUNCIL OF EUROPE COMM'R FOR HUMAN RIGHTS, DEMOCRATIC AND EFFECTIVE OVERSIGHT OF NATIONAL SECURITY SERVICES 23 (2015).

[30] For a German perspective, see Klaus Gärditz, *Legal Restraints on the Extraterritorial Activities of Germany's intelligence Services*, *in* PRIVACY AND POWER: A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA-AFFAIR 401(Russell A. Miller ed., 2016) [hereinafter Gärditz, *Legal Restraints*].

[31] *See, e.g.*, Matthias Bäcker, *Strategische Telekommunikationsüberwachung auf dem Prüfstand* [*Strategic Surveillance of Telecommunications Under Scrutiny*], 17 KOMMUNIKATION UND RECHT [K&R] 556 (2014) (Ger.); Klaus Ferdinand Gärditz, *Die Rechtsbindung des Bundesnachrichtendienstes bei Auslandstätigkeiten* [*Legal Obligations of the Federal Intelligence Service Concerning Activities Abroad*], 48 DIE VERWALTUNG 463 (2015) (Ger.) [hereinafter Gärditz, *Rechtsbindung*]; Klaus Ferdinand Gärditz, *Die Reform des Nachrichtendienstrechts des Bundes: Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes und Stärkung des Parlamentarischen Kontrollgremiums* [*The Reform of Federal Intelligence Law: The Collection of Foreign-Foreign Communications Intelligence by the Federal Intelligence Service and the Strengthening of the Parliamentary Control Panel*], 132 DEUTSCHES VERWALTUNGSABLATT [DVBL] 525 (2017) (Ger.); Sven Hölscheidt, *Das neue Recht des Bundesnachrichtendienstes* [*The New Law for the Federal Intelligence Service*], 39 JURISTISCHE AUSBILDUNG [JURA] 148 (2017) (Ger.); Christian Marxsen, *Strategische Fernmeldeaufklärung: Neuerungen in den Kompetenzen des Bundesnachrichtendienstes* [*Strategic Surveillance: Innovations in the Competencies of the Federal Intelligence Service*], 71 DIE ÖFFENTLICHE VERWALTUNG [DÖV] 218 (2018) (Ger.); Hans-Jürgen Papier, *Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten* [*Restrictions on the Freedom of Telecommunications by the Federal Intelligence Service at Data Exchange Points*], 35 NEUE ZEITSCHRIFT FÜR

these matters, especially within Europe and across the Atlantic.[32] For the intelligence law community in Germany it is important to learn how other States regulate the activities of their intelligence services. Vice versa, German intelligence legislation could be an interesting blueprint for further comparative studies because it is rather detailed and has some unique features, such as the provisions on the surveillance of EU institutions, EU Member States, and EU citizens. David Cole and Federico Fabbrini argued that there were few differences between the United States and the European Union as far as legal restrictions on State surveillance were concerned.[33] In particular, Cole and Fabbrini assumed that privacy protections on both sides of the Atlantic mainly applied territorially, to the benefit of citizen residents, with few if any legal limits constraining the capacity of intelligence agencies to conduct surveillance of foreign nationals outside their borders. In substantiating their findings, Cole and Fabbrini concentrated on the protection of privacy and personal data under EU law and the European Convention on Human Rights. They did not, however, examine the national legislation of individual EU countries. It would thus be interesting to find out whether those few States that have been identified by the FRA as having in place a more or less detailed legislation on strategic surveillance in fact distinguish between different categories of persons based on nationality and location.[34] This Article will show that German intelligence law definitely draws a distinction in this regard.

The analysis in part B begins with an examination of the statutory legal framework governing the strategic surveillance activities of the BND. It will be shown that the new provisions on the collection of signals intelligence concerning foreigners abroad provide the BND with greater leeway than the provisions that regulate the monitoring of international communications involving German nationals or foreigners staying in Germany. In part C, the focus will be on the constitutional law dimension of strategic surveillance by the BND. In particular, it needs to be examined whether the basic rights enshrined in the Basic Law

---

VERWALTUNGSRECHT [NVwZ] 1 (2016) (Ger.); CHRISTIAN SCHALLER, KOMMUNIKATIONSÜBERWACHUNG DURCH DEN BUNDESNACHRICHTENDIENST: RECHTLICHER RAHMEN UND REGELUNGSBEDARF [SURVEILLANCE OF COMMUNICATIONS BY THE FEDERAL INTELLIGENCE SERVICE: LEGAL FRAMEWORK AND THE NEED FOR REGULATION] STIFTUNG WISSENSCHAFT UND POLITIK [SWP] SWP-Studie No. 7/2016 (2016) (Ger.), https://www.swp-berlin.org/fileadmin/contents/products/studien/-2016S07_slr.pdf; SCHALLER, *supra* note 9.

[32] For a comparative perspective, see, e.g., Russell A. Miller, *A Rose by any Other Name? The Comparative Law of the NSA-Affair*, *in* PRIVACY AND POWER: A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA-AFFAIR 63 (Russell A. Miller ed., 2016). *See also* Konrad Lachmayer & Norman Witzleb, *The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective*, 37 U.N.S.W. L.J. 748 (2014) (Austl.); Joel R. Reidenberg, *The Data Surveillance State in the United States and Europe*, 49 WAKE FOREST L. REV. 583 (2014); Ronald Sievert, *The Foreign Intelligence Surveillance Act of 1978 Compared with the Law of Electronic Surveillance in Europe*, 43 AM. J. CRIM. L. 125 (2016).

[33] David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders*, 14 INT'L J. CONST. L. 220 (2016).

[34] For an overview, see FRA, FIELD PERSPECTIVES AND LEGAL UPDATE, *supra* note 20, at 43–8

(*Grundgesetz*)[35] also apply extraterritorially to the benefit of non-German nationals who are affected by the activities of the BND. The concluding observations in part D will touch upon the practicability of the existing law. Among other things, it will be held that in the age of the Internet it is practically impossible to maintain a strict separation between different types of communication based on the nationality and location of the participants. Beyond the scope of this Article are the problems of intelligence oversight (where necessary, the relevant structures are briefly described)[36] as well as the EU law and international law dimension of communications surveillance.[37]

B. Strategic Surveillance Under German Intelligence Law

The legal basis for strategic surveillance by the BND is contained in the G10 Act[38] and the BND Act.[39] The G10 Act originally dates to 1968[40] and was completely revised in 2001; the BND Act of 1990 was substantially amended in December 2016.[41] The purpose of the G10 Act is to regulate intelligence surveillance measures that qualify as restrictions of Article 10 of the Basic Law (guaranteeing the privacy of correspondence, posts, and telecommunications), whereas the BND Act governs the organization, tasks, and competences of the BND with a specific focus on the collection, processing, and use of personal data beyond the purview of Article 10. Although at first glance it seems that both Acts simply address distinct facets of the work of the BND, the German legislator has in fact established two completely different legal regimes for surveillance, which apply to different

[35] GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND [GG] [BASIC LAW], *translation at* https://www.gesetze-im-internet.de/englisch_gg/ [hereinafter Basic Law].

[36] On this subject, see Jan-Hendrik Dietrich, *Of Toothless Windbags, Blind Guardians and Blunt Swords: The Ongoing Controversy About the Reform of Intelligence Services Oversight in Germany*, 31 INTELLIGENCE & NAT'L SECURITY 397 (2016); Russell A. Miller, *Intelligence Oversight—Made in Germany*, *in* GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY 257 (Zachary K. Goldman & Samuel J. Rascoff eds., 2016).

[37] On this subject, see Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. OF INT'L L. 291 (2015); Milanovic, *supra* note 14.

[38] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses [Artikel-10 Gesetz, G 10] [Act on Restricting the Privacy of Correspondence, Posts, and Telecommunications] [G10 Act], June 26, 2001, BGBL. I at 1254, 2298, last amended by Gesetz [G], Aug. 14, 2017 BGBL. I at 3202 (Ger.).

[39] Gesetz über den Bundesnachrichtendienst [BND-Gesetz, BNDG] [Federal Intelligence Service Act] [BND Act], Dec. 20, 1990, BGBL. I at 2954, 2979, last amended by Gesetz [G], June 30, 2017 BGBL. I at 2097 (Ger.).

[40] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses [Artikel-10 Gesetz, G 10] [Act on Restricting the Privacy of Correspondence, Posts, and Telecommunications] [G10 Act], Aug. 13, 1968, BGBL. I at 949 (Ger.).

[41] Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes [Act on the Collection of Foreign-Foreign Communications Intelligence by the Federal Intelligence Service], Dec. 23, 2016, BGBL. I at 3346 (Ger.).

categories of persons depending on their nationality and location. The result is a rather fragmented legal framework.

I. Background

The evolution of German intelligence surveillance law has to be understood in light of the specific historical context following World War II.[42] The BND was founded in 1956. It replaced an organization that had been established under U.S. supervision after the end of the war. This organization had become known as *Organisation Gehlen*, named after its leader Reinhard Gehlen, a former Major General of the German *Wehrmacht*.[43] The task of *Organisation Gehlen* was to pool all available intelligence regarding the Soviet Union and its allies in Central and Eastern Europe. In 1956, the Federal Chancellery integrated this unit into the newly formed BND. Until the end of the 1960s, the activities of the BND were regulated only internally because it was widely understood that the collection of information did not interfere with any basic rights.[44] Moreover, it was presumed that such collection would largely take place outside German territory where the German Basic Law would not be applicable.[45] Germany's transition from an occupied State to full sovereignty, however, made it necessary to vest the new security institutions in Germany with sufficient legal authority to guarantee the security of the State and of those armed forces of the Three Powers (USA, United Kingdom, and France) that remained stationed in Germany after the end of the occupation regime.[46] Originally, the Three Powers enjoyed certain privileges to protect their armed forces in Germany, including the right to restrict the privacy of correspondence, posts, and telecommunications.[47] In 1968, however, the *Bundestag* adopted a constitutional reform dealing with emergency situations and the state of defense (*Notstandsverfassung*) to replace the rights of the Three Powers and to enable Germany to live up to its new sovereign status.[48] As part of this reform, a new sentence was inserted in

[42] *See generally* Gärditz, *Legal Restraints*, *supra* note 30, at 402–04 (elaborating on the origins of German intelligence legislation).

[43] Christoph Gusy, *Gesetz über den Bundesnachrichtendienst*, *in* SICHERHEITSRECHT DES BUNDES 1261 (Wolf-Rüdiger Schenke, Kurt Graulich & Josef Ruthig eds., 2014) (illustrating the historical origins of the BND).

[44] *Id.* at 1262.

[45] *Id*.

[46] Convention on Relations between the Three Powers and the Federal Republic of Germany art. 5(2), May 26, 1952, 6 U.S.T. 4251, 331 U.N.T.S. 327.

[47] Entwurf eines Gesetzes zur Ergänzung des Grundgesetzes [Draft Act Amending the Basic Law], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] V/1879, at 12–3, 17 (Ger.) (summarizing the legal status of the Three Powers in Germany before the adoption of the *Notstandsverfassung*).

[48] Siebzehntes Gesetz zur Ergänzung des Grundgesetzes [Seventeenth Law Amending the Basic Law], June 24, 1968, BGBL. I at 709 (Ger.).

Article 10(2) of the Basic Law, which paved the way for enacting legislation on secret surveillance.[49] On that basis, the *Bundestag* adopted the G10 Act in 1968.[50] The G10 Act empowers the BND, the domestic intelligence services, and the Military Counter-Intelligence Service to take, within strict legal boundaries, surveillance measures that interfere with Article 10 of the Basic Law. Section 3(1) of the G10 Act allows for the targeted surveillance of individual communications with a view to preventing or prosecuting certain serious criminal offenses (*Beschränkungen in Einzelfällen*); Section 5(1) authorizes the BND to monitor international telecommunications relations for the purpose of identifying or countering certain enumerated threats (*strategische Beschränkungen*).[51] Over the years, the G10 Act has been amended several times to accommodate new threats, such as international terrorism, different forms of transnational organized crime, and cyberattacks. In 1999, the Federal Constitutional Court (*Bundesverfassungsgericht*) found that some provisions in the G10 Act were not compatible with the Basic Law.[52] Therefore, the *Bundestag* completely revised the G10 Act in 2001.[53]

Another important factor in the evolution of German intelligence law was the growing public awareness for data protection during the 1980s. In the *Census Act Case* (*Volkszählungsurteil*) of 1983, the Federal Constitutional Court emphasized that restrictions on the right to informational self-determination were admissible only on a clear statutory basis.[54] In 1990, the *Bundestag*, after several years of unsuccessful negotiations, finally passed a package of laws that regulate the collection, processing, and use of personal data for intelligence

[49] Basic Law, art. 10(2)2: "If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a *Land*, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature."

[50] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses [Artikel-10 Gesetz, G 10] [Act on Restricting the Privacy of Correspondence, Posts, and Telecommunications] [G10 Act], Aug. 13, 1968, BGBL. I at 949 (Ger.). *See generally* Berthold Huber, *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, *in* SICHERHEITSRECHT DES BUNDES 1349–51 (Wolf-Rüdiger Schenke, Kurt Graulich & Josef Ruthig eds., 2014) (illustrating the evolution of the G10 Act).

[51] *See infra* note 62 and accompanying text.

[52] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 100 BVERFGE 313 (Ger.). For a summary of this case, see DONALD P. KOMMERS & RUSSEL A. MILLER, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 414–15 (3d ed. 2012).

[53] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses [Artikel-10 Gesetz, G 10] [Act on Restricting the Privacy of Correspondence, Posts, and Telecommunications] [G10 Act], June 26, 2001, BGBL. I at 1254, 2298, last amended by Gesetz [G], Aug. 14, 2017 BGBL. I at 3202 (Ger.).

[54] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 65 BVERFGE 1 (44) (Ger.). *See Infra* notes 155, 160 and accompanying text.

purposes.[55] Part of this package was the BND Act, which has also been amended several times since its adoption.[56] The BND's mandate, according to Section 1(2)1 of the BND Act, is to collect and analyze information necessary for obtaining intelligence on foreign countries that is relevant for the foreign and security policy of the Federal Republic of Germany.[57] The collection of intelligence on domestic matters is not part of its mandate, even if there is a link to international developments.[58] Surveillance of purely domestic communications falls into the competence of the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*, BfV) and of the sixteen federal states authorities for the protection of the constitution (*Landesämter für Verfassungsschutz*, LfVs). Section 2(3) of the BND Act stipulates that the BND has no police powers and is generally prevented from requesting enforcement action from the police. This rule is an expression of the *Trennungsgebot*, which is an important principle of German security law. It means, *inter alia*, that the police and the intelligence services have clearly distinct functions, mandates, and powers, that they are organized separately, and that the exchange of information between both spheres is strictly limited. In the fight against international terrorism, however, the lines of separation have become blurred and contested due to increased cooperation between the different authorities.[59]

II. Differentiations in German Intelligence Law: The Dichotomy Between G10 Communications and Routine Communications

It has already been mentioned above that the purpose of the G10 Act is to regulate surveillance measures that qualify as restrictions of Article 10 of the Basic Law. But the crux of the matter is that the Federal Government and the BND firmly hold the view that Article 10 exclusively protects German nationals and domestic legal persons (irrespective of their

---

[55] Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes [Act on the Further Development of Data Processing and Data Protection], Dec. 20, 1990, BGBL. I at 2954 (Ger.).

[56] Some provisions contained in the BND Act are rather unspecific. The exact legal consequences of their application can be identified only in conjunction with the more comprehensive and detailed provisions of another law to which the BND Act extensively refers: Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz [BVerfSchG] [Act on Cooperation Between the Federation and the Federal States in Matters Relating to the Protection of the Constitution, and on the Federal Office for the Protection of the Constitution], Dec. 20, 1990, BGBL. I at 2954, 2970, last amended by Gesetz [G], June 30, 2017 BGBL. I at 2097 (Ger.).

[57] BND Act § 1(2)1.

[58] Gesetzesentwurf der Bundesregierung [Draft Act by the Federal Government], BUNDESRAT: DRUCKSACHEN [BR] 618/88, at 183 (commenting on BND Act § 1).

[59] *See generally* Michael Lysander Fremuth, *Wächst zusammen, was zusammen gehört? Das Trennungsgebot zwischen Polizeibehörden und Nachrichtendiensten im Lichte der Reform der deutschen Sicherheitsarchitektur* [*What Belongs Together Grows Together? The Principle of Separation Between Law Enforcement Authorities and Intelligence Services in Light of the Reform of German Security Architecture*], 139 ARCHIV DES ÖFFENTLICHEN RECHTS [AÖR] 32 (2014) (Ger.).

location), as well as non-German nationals staying within the territory of the Federal Republic of Germany.[60] According to this restrictive understanding, the communication of non-German nationals who are outside of Germany is not protected by Article 10 of the Basic Law and does therefore not fall under the G10 Act. The BND thus distinguishes between so-called "G10 communications" (international communications that involve at least one participant who is considered to be entitled to protection by Article 10 of the Basic Law)[61] and "routine communications" (communications involving only foreigners abroad, *Ausland-Ausland-Fernmeldeaufklärung*). While G10 communications may be subject to strategic surveillance under the strict conditions established by the G10 Act, the monitoring of routine communications is permissible according to the BND Act under conditions that are far less restrictive. This dichotomy also plays an important role with regard to the processing and use of related personal data. A particularly sensitive aspect is the transfer of personal data to foreign intelligence services. The different legal regimes will now be briefly contrasted.

1. Strategic Surveillance of G10 Communications

The following overview shows that the surveillance of G10 communications is subject to rather restrictive conditions that are supposed to guarantee a fairly high level of privacy protection in accordance with Article 10 of the Basic Law:

- *Threshold:* Section 5(1) of the G10 Act authorizes the BND to monitor international telecommunications relations exclusively for the purpose of identifying or countering certain enumerated security threats. The list comprises the following threats: Armed attack against Germany; international terrorist attack with a direct link to Germany; international proliferation of certain weapons, related goods, computer programs, and technologies; organized drug trafficking into the EU with a link to Germany; interference with the currency stability in the Euro-zone through counterfeiting; internationally organized money-laundering; organized smuggling of foreign nationals into the EU with a link to Germany; certain cyberattacks with a link to Germany.[62]

[60] *See* Kurt Graulich, Nachrichtendienstliche Fernmeldeaufklärung mit Selektoren in einer transnationalen Kooperation [Signals Intelligence and the Use of Selectors in Transnational Cooperation], Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode [1st Committee of Inquiry of the 18th Legislative Period], Doc. MAT A SV-11/2 on A-Drs. 404, Oct. 23, 2015, at 44 (Ger.) [hereinafter Graulich Report] (summarizing the legal views of the BND). The position of the Federal Government is summarized in 100 BVERFGE 313 (338–39) (Ger.).

[61] The notion "international telecommunications relations" in Section 5(1) of the G10 Act is interpreted by the Federal Government and the BND to include only cross-border communications to and from Germany, not communications where all participants are located abroad. *See* Gesetzesentwurf der Bundesregierung [Draft Act by the Federal Government], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 14/5655, at 18 (Ger.) (commenting on G10 Act § 5(1)1, 2); Antwort der Bundesregierung [Response by the Federal Government], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 17/9640, at 6 (Ger.) (summarizing the scope of application of the G10 Act).

[62] In 1999, the Federal Constitutional Court ruled that the threats listed in the predecessor provision of Section 5(1) in the 1994 version of the G10 Act was sufficiently specific and precise. In the view of the Court, a further

- *Procedure and formal requirements:* According to Section 5(1) of the G10 Act, the BND must request an order for strategic surveillance from the Federal Ministry of the Interior. Such an order, which has to determine the specific parameters of the measure,[63] may allow the BND, for renewable terms of no more than three months,[64] to monitor and record communications that are transmitted to and from Germany through certain cables or satellite channels. The measure must be immediately stopped if it is not necessary anymore or if the conditions for the order are not fulfilled anymore.[65] Every order requires approval by the Parliamentary Control Panel.[66]

- *Specific Precautions:* In terms of basic rights protection, the G10 Act provides for specific precautions to safeguard the inviolable core area of private life (*Kernbereich privater Lebensgestaltung*). The Federal Constitutional Court decided that an encroachment upon the core area of private life by way of surveillance could not even be justified in the interest of the greater public good.[67] Subject to absolute protection are perceptions, feelings, considerations, views, and experiences of a highly personal character. Accordingly, it is stipulated in the G10 Act that the BND must not use search terms that relate to the core area of private life.[68] If there is reasonable ground to believe that an act of surveillance will lead to information relating to this core area, the measure must be stopped. As far as such information is generated accidentally, it may not be used and must be immediately erased.[69] It is noteworthy, however, that the prohibition on the use of search terms that relate to the core area of private life does not apply to matters concerning foreigners abroad. Outside the territory of the Federal Republic of Germany, only German nationals benefit from this particular prohibition.[70] Aside from that, the BND is generally not permitted in a strategic surveillance operation to use search terms

clarification of the conditions for taking surveillance measures was not possible due to the specific character of the tasks and working methods of the BND. *See* 100 BVERFGE 313 (372–73) (Ger.).

[63] G10 Act § 10(2), (4).

[64] G10 Act § 10(5).

[65] G10 Act § 11(2).

[66] G10 Act §§ 5(1), 14.

[67] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 34 BVERFGE 238 (245); 109 BVERFGE 279 (313); 120 BVERFGE 274 (335) (Ger.). *See also infra* note 147 and accompanying text.

[68] G10 Act § 5(2)2(lit. 2).

[69] G10 Act § 5a.

[70] G10 Act § 5(2)2(lit. 2), (2)3.

that would directly lead to the phone or computer of a German national.[71] The purpose of this provision is to protect German nationals from targeted monitoring conducted under the cover of a strategic surveillance order.[72]

- *Data Protection:* Personal data that has been collected on the basis of Section 5(1) of the G10 Act is specifically protected. In particular, the BND is obliged to evaluate on a continuous basis which data is necessary to fulfill its tasks. Data that is not necessary must be immediately erased.[73] All remaining data must be earmarked and may be used only for enumerated purposes.[74]

- *Obligation to notify affected persons:* A person affected by surveillance measures under Section 5(1) of the G10 Act must generally be informed after completion of the measures.[75] This obligation, however, is qualified by several exemptions.[76]

- *Involvement of the G10 Commission:* Because ongoing strategic surveillance measures under Section 5(1) are not open to judicial review by a court,[77] the G10 Act establishes an alternative review mechanism involving the G10 Commission.[78] This Commission decides ex officio or upon complaint whether a specific surveillance measure is admissible and necessary. Its control mandate also extends to the processing and use of personal data under the G10 Act. If the G10 Commission deems a surveillance order to be inadmissible or unnecessary, the Federal Ministry of the Interior must immediately revoke the order.

---

[71] G10 Act § 5(2)2(lit. 1), (2)3.

[72] Gesetzesentwurf der Bundesregierung [Draft Act by the Federal Government], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 14/5655, at 20 (Ger.) (commenting on G10 Act § 5(2)3).

[73] G10 Act § 6(1).

[74] G10 Act § 6(2).

[75] G10 Act § 12(2).

[76] Notification is excluded as long as it cannot be ruled out that the purpose of the measure would be jeopardized or as long as it is to be expected that such notification would have negative consequences for the wellbeing of the country. After twelve months without notification, the G10 Commission has to make a decision on the matter. *See* G10 Act § 12(2).

[77] G10 Act § 13.

[78] The G10 Commission was created by the G10 Act. Its organization and procedure are regulated in Section 15 of the G10 Act. The members of the Commission are appointed by the Parliamentary Control Panel. They are completely independent.

2. Surveillance of Routine Communications

For a long time, the BND monitored the communication of foreigners abroad without explicit statutory authorization.[79] The new rules on *Ausland-Ausland-Fernmeldeaufklärung* of December 2016 that have been included in the BND Act are supposed to enhance legal certainty by providing the BND with a specific statutory basis for such action. Critics, however, say that the real purpose of the reform was to legalize long-standing BND practices.[80]

Section 6(1) of the BND Act now authorizes the BND (within Germany)[81] to process personal data collected from telecommunication networks through which *Ausland-Ausland* communications are transmitted. Section 6(4) of the BND Act makes clear that this authorization does not cover the collection of data from communications involving German nationals, domestic legal persons, or foreign nationals staying in Germany (G10 communications). As far as such data is collected as a by-catch, it has to be immediately erased unless there is a separate order for surveillance under the G10 Act.[82] To segregate G10 communications from routine communications, the BND employs special filter programs.[83]

---

[79] The BND has always relied on Section 1(2)(1) of the BND Act, which merely defines its task in very general terms. *See* Antwort der Bundesregierung [Response by the Federal Government], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 17/9640, at 10 (Ger.) (summarizing the Federal Government's legal view); Gesetzesentwurf der Fraktionen der CDU/CSU und SPD [Draft Act by the Parliamentary Groups CDU/CSU and SPD], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/9041, at 1 (Ger.). *See also* 100 BVerfGE 313 (380) (Ger.) (summarizing the legal view of the BND). *See also* Bäcker, *supra* note 31, at 559–60 (criticizing the position of the Federal Government and the BND concerning Section 1(2)1 of the BND Act).

[80] *See, e.g.*, Jörg Diehl & Annett Meiritz, *BND darf künftig manchmal immer fast alles vielleicht* [BND Is Perhaps Allowed to Do Almost Everything Sometimes Always], SPIEGEL ONLINE (July 8, 2016), http://www.spiegel.de/politik/deutschland/bnd-reform-des-deutschen-geheimdienstes-im-eiltempo-a-1101891.html (quoting Nikolaos Gazeas).

[81] Section 6(1) of the BND Act applies only to operations conducted by the BND from within German territory. An explanatory note on the draft legislation states that this is the case insofar as the systems employed by the BND are located on German soil. Outside Germany, the BND continues to operate solely on the basis of Section 1(2)(1) of the BND Act. With regard to such extra-territorial operations, the new Section 7 of the BND Act contains a lex specialis rule on the processing and use of personal data. *See* Gesetzesentwurf der Fraktionen der CDU/CSU und SPD [Draft Act by the Parliamentary Groups CDU/CSU and SPD], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/9041, at 22 (Ger.).

[82] *Id*.

[83] *See id.* at 24 (describing the use of filters for the purpose of sorting out protected G10 communications). *See also* Report of the 1st Committee of Inquiry, *supra* note 3, at 898–901.

The following lineup serves to demonstrate that the conditions for the surveillance of communications of foreigners abroad (and for the handling of related personal data) are far more permissive than the standards contained in the G10 Act.

- *Lower threshold:* In contrast to Section 5(1) of the G10 Act, Section 6(1) of the BND Act does not require that the measure serves the purpose of identifying or countering a specified threat (armed attack, terrorist attack, proliferation, etc.). Instead, Section 6(1) of the BND Act merely demands that the data are necessary to identify and counter "threats to the Federal Republic of Germany's internal or external security," to ensure the Federal Republic of Germany's capability to act, or to obtain other intelligence that is relevant for the foreign and security policy of the Federal Republic of Germany on matters determined by the Federal Government.[84] The vagueness of this provision may be considered as being in line with the relatively broad mandate of the BND formulated in Section 1(2)(1) of the BND Act, which is to provide the Government with a wide variety of strategically relevant information, including information on economic developments, in the field of foreign and security policy.[85] Germany's foreign and security policy interests are defined and prioritized for the BND by the Federal Chancellery in consultation with other federal ministries in a mission profile (*Auftragsprofil*).[86] The executive branch in Germany has a core area of responsibility where it can make its decisions largely independent from the parliament (*Kernbereich exekutiver Eigenverantwortung*).[87] This follows from the principle of the separation of powers (Article 20(2)(2) of the Basic Law). The leeway of the Federal Government is particularly broad in the domain of foreign policy.[88] In October 2016, for instance, the Federal Constitutional Court decided that the Federal Government had not violated the rights of the *Bundestag* by refusing to submit a list of NSA selectors to the Committee of Inquiry.[89] In this case, the Court reaffirmed that it is part of the responsibility of the Government to determine the strategic parameters for the work of the intelligence

[84] BND Act § 6(1)1.

[85] *See* Gesetzesentwurf der Fraktionen der CDU/CSU und SPD [Draft Act by the Parliamentary Groups CDU/CSU and SPD], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/9041, at 22 (Ger.) (commenting on BND Act § 6(1)).

[86] Notification by the Parliamentary Control Panel, *supra* note 7, at 5 (describing the character of the *Auftragsprofil*).

[87] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 67 BVERFGE 100 (139); 110 BVERFGE 199 (214); 124 BVERFGE 78 (120); 131 BVERFGE 152 (206); 137 BVERFGE 185 (234) (Ger.).

[88] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 40 BVERFGE 141 (178); 55 BVERFGE 349 (365) (Ger.).

[89] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], 2 BvE 2/15, Oct. 13, 2016, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/10/-es20161013_2bve000215.html (Ger.).

services and to guarantee their operational capability.[90] Although Section 6(1) of the BND Act, with its broad wording, takes account of that responsibility, it is questionable whether the provision would stand the constitutional law test of determinedness[91] if scrutinized by the Federal Constitutional Court—especially if the Court would recognize that Section 6(1), just like Section 5(1) of the G10 Act, could serve as a legal basis for actions that interfere with Article 10 of the Basic Law.

- *Relaxed procedure and formal requirements:* Responsibility for issuing surveillance orders under the BND Act lies with the Federal Chancellery; the Parliamentary Control Panel, however, is not involved in this process.[92] While an order for surveillance under Section 5(1) of the G10 Act requires expressly listing the search terms,[93] orders under Section 6(1) of the BND Act may generally be issued without such specification.[94] Moreover, orders under Section 5(1) of the G10 Act must identify a target area (geographic region or certain States), certain transmission channels, and a certain percentage of the capacity of these channels that shall be subject to strategic surveillance (not exceeding 20 percent).[95] No such restrictions exist under the BND Act.[96] Finally, an order under Section 6(1) of the BND Act may allow the BND to take such measures for renewable terms of nine months (not just three months).[97]

- *No obligation to notify affected persons:* The BND generally has no obligation to inform persons affected by measures taken on the basis of Section 6(1) of the BND Act. An obligation to notify arises only insofar as such measures have accidentally produced (in

[90] *Id.* at para. 127.

[91] *See Infra* note 163 and accompanying text.

[92] BND Act § 9.

[93] G10 Act § 10(4).

[94] BND Act § 9(1). Paragraph 2 stipulates that the use of search terms that directly lead to EU institutions or authorities of EU Member States require a separate order.

[95] G10 Act § 10(4).

[96] The order must identify only the relevant telecommunication network. *See* BND Act § 6(1)2, § 9(1)2 (lit. 2). But the notion "telecommunication network" is fairly broad under German telecommunication law. *See* Gesetzesentwurf der Fraktionen der CDU/CSU und SPD [Draft Act by the Parliamentary Groups CDU/CSU and SPD], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/9041, at 22–3 (Ger.) (commenting on this notion).

[97] BND Act § 9(3).

violation of Section 6(4) of the BND Act) data relating to German nationals, domestic legal persons, or foreign nationals staying in Germany.[98]

- *Lower standards for data protection:* Like the G10 Act, the BND Act contains a general provision on the protection of the core area of private life.[99] But the hurdles for the storage of personal data (in particular traffic data) are significantly lower than those established by the G10 Act.[100] An area where the dichotomy between G10 communications and routine communications is highly relevant is the transfer of personal data to foreign intelligence services, which will be addressed separately below.

- *No involvement of the G10 Commission:* Instead of empowering the G10 Commission to control the BND's activities in the field of *Ausland-Ausland-Fernmeldeufklärung*,[101] the BND Act provides for the creation of a new body, the so-called "Independent Panel" (*Unabhängiges Gremium*).[102] This Panel is filled with judges of the Federal Court of Justice and a Federal Public Prosecutor. Its task is to examine whether an order for surveillance is admissible and necessary.[103] If it declares a surveillance order to be inadmissible or unnecessary, the order must be immediately revoked. The procedure is similar to the G10 Commission procedure under the G10 Act. The BND Act, however, does not explicitly vest the Independent Panel with authority to exercise control over the entire processing and use of personal data.[104] A main difference between the G10 Commission and the Independent Panel is that the members of the latter body are appointed by the Federal Government and not by the Parliamentary Control Panel of the *Bundestag*.[105] This is a somewhat strange construction given the fact that the parliament traditionally plays an important role in controlling the intelligence services in Germany.

---

[98] BND Act § 10(4). In this case, as far as German nationals, domestic legal persons, or foreign nationals staying in Germany are concerned, the procedure for notification is the same as the procedure envisioned in Section 12 of the G10 Act.

[99] BND Act § 11.

[100] BND Act §§ 6(6), 10, 19, 20.

[101] The G10 Commission will only be involved in exceptional circumstances—if a measure of surveillance under Section 6(1) of the BND Act accidentally leads to the collection of data relating to German nationals, domestic legal persons, or foreign nationals staying in Germany (BND Act § 10(4)).

[102] BND Act § 16.

[103] BND Act § 9(4). *See also* § 9(5).

[104] Additional competences of the Independent Panel are provided by Section 15(3) of the BND Act.

[105] BND Act § 16(2).

3. The Transfer of Personal Data to Foreign Intelligence Services

The exchange of information between intelligence services at the international level is of paramount importance for countering terrorist attacks committed by persons who are highly mobile and well connected across the globe. Timely information about terrorist plots and suspected perpetrators is probably the most valuable currency in the business of intelligence cooperation today. The principle of reciprocity[106] means that an intelligence service may only expect to receive insights about such plots from foreign services if it also delivers such information. This implies that the BND must have sufficient authority and power to cooperate on a level playing field with the NSA and other foreign intelligence services.

The transfer of personal data to foreign intelligence services, however, is a particularly sensitive matter because there is usually no guarantee that the data will be processed and used by the receiving State in compliance with fundamental human rights norms. The G10 Act addresses this problem by establishing strict conditions for the transfer of personal data by the BND. These conditions are defined in Section 7a of the G10 Act. In particular, the transfer must not conflict with overriding individual rights of the affected person. Permissible transfers require adequate data protection standards to apply in the receiving State.[107] In a judgment of April 2016, which deals with the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz*), the Federal Constitutional Court further specified the constitutional law requirements for the transfer of personal data to foreign authorities.[108] In this regard, the Court referred to the 2015 judgment of the Court of Justice of the European Union in *Schrems*[109] and insisted that there shall be an "adequate" level of data protection in the receiving State, which does not need to be identical with or equivalent to the German standards, but which must ensure that human rights norms will not be undermined.[110] Under no circumstances may Germany be complicit in violations of human dignity.[111]

---

[106] *See, e.g.*, G10 Act § 7a(1)1(lit. 3).

[107] G10 Act § 7a(1)1(lit. 2). On the meaning of the term "*Rechtsstaat*", which has no exact equivalent in the English language, see KOMMERS, *supra* note 52, at 48.

[108] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], 1 BvR 966/09, 1 BvR 1140/09, Apr. 20, 2016, paras. 323–41, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/-DE/2016/04/rs20160420_1bvr096609.html (Ger.).

[109] Case C-362/14, Schrems v. Data Protection Commissioner/Digital Rights Ireland Ltd. (Oct. 6, 2011), http://curia.europa.eu.

[110] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], BVerfG, 1 BvR 966/09, 1 BvR 1140/09, Apr. 20, 2016, paras. 334–5, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/-DE/2016/04/rs20160420_1bvr096609.html (Ger.).

[111] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], BVerfG, 2 BvR 2735/14, Dec. 15, 2015, para. 62, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2015/12/-rs20151215_2bvr273514.html; BVerfG, 1 BvR 966/09, 1 BvR 1140/09, Apr. 20, 2016, para. 328,

Procedurally, every transfer of personal data under Section 7a of the G10 Act is to be authorized by a qualified lawyer of the BND and approved by the Federal Chancellery.[112] The data must be earmarked and the details of the transfer must be documented in the records.[113] In addition, the BND shall obtain from the receiving intelligence service a binding commitment that the data will be used only for the purpose of the transfer, that the earmarking of the data will be kept, and that the BND will, upon request, be informed of the further use of the data.[114] Moreover, the G10 Commission and the Parliamentary Control Panel must be notified of each transfer.[115] Under such strict conditions, the hurdles for the transfer of personal data to foreign intelligence services are rather high and the procedure is complex and time-consuming.

As far as the transfer of personal data from routine communications is concerned, the BND Act provides the BND with greater flexibility. Under the BND Act, such transfer is generally not subject to control by the G10 Commission. Over the years, a legal practice has evolved according to which the BND transferred personal data to the NSA by simply invoking Section 1(2)(1) of the BND Act as a legal basis—and without considering itself bound by any specific statutory limitations.[116] This practice has been rightly criticized because Section 1(2)(1) of the BND Act describes only the general mandate of the BND and does not contain any language that could be interpreted as a legal authorization for the transfer of personal data.[117] The 2016 reform of the BND Act has provided the BND with explicit competences in this field. Section 15 of the BND Act allows for an automated transfer of personal data to the authorities of another State within a formalized framework of cooperation. The conditions for the establishment of a formalized institutional cooperation with foreign intelligence

---

http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/-DE/2016/04/rs20160420_1bvr096609.html (Ger.).

[112] G10 Act § 7a(1)2, (3)1.

[113] G10 Act §§ 6(2), 7a(3)2–4.

[114] G10 Act § 7a(4).

[115] G10 Act § 7a(5), (6).

[116] Öffentliche Zeugenvernehmung [Testimony] Frau RDn Dr. H. F., Bundesnachrichtendienst, Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode [1st Committee of Inquiry of the 18th legislative period], Stenographisches Protokoll der 16. Sitzung, vorläufige Fassung [Stenographic Transcript, 16th Session, preliminary version], Oct. 9, 2014, at 11, 29, 72, https://wikileaks.org/bnd-nsa/sitzungen/16/-WikiLeaks_Transcript_Session_16_from_German_NSA_Inquiry.pdf (noting that the BND considered itself bound in such cases only by the fundamental principles of the *Rechtsstaat*, in particular by the guarantee of human dignity, the prohibition on arbitrary action, and the principle of proportionality). *See also* SCHALLER, *supra* note 31, at 35–36 (summarizing the line of argument pursued by the BND).

[117] Bäcker, *supra* note 31, at 559–60 (arguing that Section 1(2)1 of the BND Act could not serve as a legal basis for action within the scope of Article 10 of the Basic Law); SCHALLER, *supra* note 31, at 32. *See also infra* note 163 and accompanying text.

services are defined in Section 13 of the BND Act. This provision stipulates that the details of the cooperation have to be put down in a memorandum of understanding, which needs to be approved by the Federal Chancellery and notified to the Parliamentary Control Panel.[118] Once the cooperation is established, the door is more or less open for an automated transfer of data that has been collected within the framework of this particular cooperation.[119] Moreover, the BND may also maintain data sets to which public authorities of other States have access for the purpose of exchanging or analyzing intelligence related to certain threat situations or certain groups of persons; and it may participate in such projects undertaken by foreign authorities.[120] This is another form of highly institutionalized cooperation. Apart from that, however, the BND Act does not prevent the BND from carrying on with its long-standing practice of invoking Section 1(2)(1) as a legal basis for an ad hoc exchange of information in less formalized cooperation contexts.

The exchange of data collected in the context of *Ausland-Ausland-Fernmeldeaufklärung* is probably the most important part of the BND's cooperation with the NSA and other intelligence services. If the high standards established by the G10 Act would be applied without any modification to all cases of data transfer, the cooperation between the BND and the NSA would be severely hampered. This might explain why the Federal Government and the *Bundestag* pushed for a reform of the BND Act that deals with the complex of *Ausland-Ausland-Fernmeldeaufklärung* wholly beyond the ambit of Article 10 of the Basic Law. In its decision of October 2016 dealing with the Federal Government's refusal to submit a list of NSA selectors to the Committee of Inquiry, the Federal Constitutional Court acknowledged that there is a relationship of mutual dependency between German and U.S. intelligence services.[121] In particular, the Court referred to the threats posed by international terrorism and cyberattacks. In light of these threats, the Court recognized that international intelligence cooperation is of "paramount importance" for Germany and that the

[118] BND Act § 13(3), (5).

[119] Section 15(1) of the BND Act contains additional safeguards for the protection of personal data of German nationals, EU institutions, authorities of EU Member States, and EU citizens, as well as for the protection of the national interests of the Federal Republic of Germany.

[120] BND Act §§ 26–30.

[121] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], 2 BvE 2/15, Oct. 13, 2016, para. 171, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/10/-es20161013_2bve000215.html (Ger.). In an earlier decision, the Court already stressed that an exchange of data served to maintain inter-State relations and the freedom of action of the Federal Government on the international plane. *See* BVerfG, 1 BvR 966/09, 1 BvR 1140/09, Apr. 20, 2016, para. 325, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/-rs20160420_1bvr096609.html (Ger.).

partnership with the United States is "indispensable."[122] In the view of the Court, a suspension of such cooperation could cause a permanent loss of essential intelligence on foreign and security policy matters. Moreover, the Court warned that such an impairment of the operational capability of the intelligence services, even if only temporary, would not be tolerable.[123] For the moment, it is difficult to predict what this decision could mean for further surveillance-related cases that will be brought before the Federal Constitutional Court. On the one hand, the decision sends a strong signal in favor of international intelligence cooperation. On the other hand, as will be argued in part C below, the discrimination between different categories of persons based on nationality and location is difficult to reconcile with German constitutional law.

III. "Spying on Friends": New Rules for the Surveillance of EU Institutions, EU Member States, and EU Citizens

"Spying on friends is unacceptable" ("*Ausspähen unter Freunden, das geht gar nicht"*). Those were the words of German Chancellor Angela Merkel in October 2013 reacting to reports that the NSA had tapped her cell phone.[124] Since then, it has become public knowledge that the BND had also extensively used selectors leading to the communication of EU and NATO partners.[125] A 2016 report published by the Parliamentary Control Panel of the German *Bundestag* refers to a list of about 3,300 institutions and persons that were potentially under surveillance by the BND.[126] These targets included heads of State and government of EU and NATO Member States, ministers and their staff, military facilities of such States, EU institutions, diplomatic missions with an EU/NATO link, as well as NGOs, companies (especially from the aerospace, defense, transport, media, and consultancy sectors), and certain individuals with an EU/NATO background.[127] In the media it was reported that even a high-ranking German diplomat had been monitored by the BND while working for the

---

[122] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], 2 BvE 2/15, Oct. 13, 2016, para. 171, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/10/-es20161013_2bve000215.html (Ger.).

[123] *Id.* at para. 174.

[124] *See, e.g.*, Nick Bryant, *Spying Row: Merkel Urges US to Restore Trust at EU Summit,* BBC NEWS (Oct. 25, 2013), http://www.bbc.com/news/world-europe-24647602.

[125] *Governments and NGOs—Germany Spied on Friends and Vatican*, SPIEGEL ONLINE (Nov. 7, 2015), http://www.spiegel.de/international/germany/german-bnd-intelligence-spied-on-friends-and-vatican-a-1061588.html; Martin Williams, *Germany "Spied" on John Kerry and Hillary Clinton—Der Spiegel*, THE GUARDIAN (Aug. 16, 2014), https://www.theguardian.com/world/2014/aug/16/germany-spied-john-kerry-hillary-clinton-der-spiegel.

[126] Notification by the Parliamentary Control Panel, *supra* note 7. According to the report, the BND stopped the operation of selectors relating to the listed institutions and persons in 2013.

[127] *Id.* at 8–14.

European Union.[128] When Chancellor Merkel testified before the Committee of Inquiry of the *Bundestag* in February 2017, she firmly stood by her 2013 statement that spying on friends was unacceptable.[129]

One of the most remarkable features of the 2016 reform of the BND Act is that the *Bundestag* has, for the first time, adopted specific rules for the surveillance of EU institutions, authorities of EU Member States, and EU citizens.[130] This is noteworthy for two reasons. On the one hand, it is now clearly laid down in the law that the BND in certain circumstances will also "spy on friends." On the other hand, it seemed important to the Federal Government and the *Bundestag* to make clear that the BND does not have unfettered authority in this sensitive area. Section 6(3) of the BND Act stipulates that search terms which lead to a targeted interception of the communications of such institutions or persons may be used only in two cases: (1) if necessary to identify or counter a threat listed in Section 5(1) of the G10 Act; or (2) to gain information as defined in Section 6(1) of the BND Act insofar as the measure is focused exclusively on the collection of data concerning developments in *third* States, and to the extent that these developments are of particular relevance for Germany's security.[131] Furthermore, the BND may use search terms leading to EU citizens if necessary to identify or counter certain criminal offenses within the meaning of Section 3(1) of the G10 Act.[132]

While Section 6(3) of the BND Act raises the bar for surveillance measures against EU institutions, authorities of EU Member States, and EU citizens, it does not guarantee the same standard of protection as the G10 Act. Differences remain especially with regard to the protection of personal data.[133] The German legislator has thus created a third category of communications that enjoy an intermediate level of protection. On the one hand, the surveillance of such institutions, authorities, and persons is subject to a more restrictive legal

---

[128] Michael Götschenberg, *BND hörte deutschen Diplomaten ab* [*BND Listened in on German Diplomate*], TAGESSCHAU.DE (Nov. 11, 2015), https://www.tagesschau.de/inland/bnd-selektorenliste-103.html.

[129] *Merkel vor NSA-Untersuchungsausschuss—"Ich wusste davon nichts"* [Merkel Before the Committee of Inquiry on the NSA Affair—"I Didn't Know Anything"], SPIEGEL ONLINE (Feb. 16, 2017), http://www.spiegel.de/politik/deutschland/nsa-merkel-gegen-spionage-zwischen-verbuendeten-staaten-a-114915.html.

[130] *See supra* note 12.

[131] BND Act § 6(3)1.

[132] BND Act § 6(3)2.

[133] Sections 10(3) and 15(1) of the BND Act provide that data which has been collected in violation of Section 6(3) of the BND Act must be immediately erased and may not be subject to an automated transfer to foreign intelligence services. Data that has been collected in accordance with Section 6(3) is subject to the same data protection standards as other data collected under Section 6(1), which are lower than those established by the G10 Act. *See supra* note 100.

framework than the surveillance of routine communications of other foreigners abroad.[134] On the other hand, the conditions for the surveillance of such EU communications, as well as for the processing and use of related personal data, are less restrictive than those applying to G10 communications.

Interestingly, the BND Act does not contain any restrictions regarding the surveillance of other international organizations like the United Nations or NATO. The communication of such institutions, as well as the communication of authorities of non-EU partner countries such as the United States, may be subject to strategic surveillance under the normal standards applying to routine communications as laid down in the BND Act.[135] The only limitation in this regard is contained in Section 6(2) of the BND Act, which stipulates that the use of search terms for the purpose of collecting content data (not traffic data) must always be consistent with Germany's foreign and security policy interests. In the explanatory note to this provision, it is stated that the BND shall be generally prevented from using search terms that lead to the communication of heads of States with which Germany maintains close and cooperative partnership relations.[136]

To the knowledge of the present author, Germany is the only country in Europe that has regulated these issues in a federal law. The explanatory note on the draft legislation clarifies that the aim was to enhance legal certainty.[137] It seems, however, that the Federal Government and the *Bundestag* were also driven by the desire to demonstrate that Germany is able to pursue its legitimate security interests within a transparent legal framework that respects not only the principles of the *Rechtsstaat* but also takes due account of Germany's loyalty and responsibility vis-à-vis its European partners. From an international law perspective, however, it is important to note that espionage activities directed against the authorities of foreign countries are not prohibited per se;[138] and EU law also does not regulate such activities between EU Member States.[139]

---

[134] *See* also the procedural requirements established by Section 9(2), (5) of the BND Act.

[135] On the need for a transatlantic privacy agreement, see Cole & Fabbrini, *supra* note 33, at 233–37.

[136] Gesetzesentwurf der Fraktionen der CDU/CSU und SPD [Draft Act by the Parliamentary Groups CDU/CSU and SPD], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/9041, at 23 (Ger.) (commenting on BND Act § 6(2)).

[137] *Id.* at 1.

[138] Stefan Talmon, TAPPING THE GERMAN CHANCELLOR'S CELL PHONE AND PUBLIC INTERNATIONAL LAW (Bonn Research Papers on Public International Law, Paper No. 3A/2013, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2352834.

[139] Article 4(2) of the Treaty on European Union makes clear that national security remains the sole responsibility of each Member State.

IV. Preliminary Conclusion

It has been demonstrated that German intelligence surveillance law is rather fragmented. The surveillance of electronic communications that involve at least one participant who is either a German national or a foreigner staying in Germany is regulated in the G10 Act, which guarantees a relatively high level of protection of privacy in accordance with Article 10 of the Basic Law. The monitoring of communications exclusively involving foreigners abroad, which is subject to the newly reformed BND Act, however, is permissible under conditions that are far less restrictive than those established by the G10 Act. This dichotomy between so-called "G10 communications" and "routine communications" is also relevant with regard to the protection of personal data because the G10 Act and the BND Act define completely different standards for the processing and use of such data. A particularly sensitive aspect is the transfer of personal data to foreign intelligence services. While the BND Act is rather open for the transfer of data relating to routine communications, the relevant provisions in the G10 Act are more limiting. In addition to these two categories, there is a third category of surveillance targets comprising EU institutions, authorities of EU Member States, and EU citizens, which enjoy an intermediate level of protection against surveillance under the BND Act.

By regulating the entire complex of *Ausland-Ausland-Fernmeldeaufklärung* in the BND Act and not in the G10 Act—and by scrupulously avoiding in the BND Act any reference to Article 10 of the Basic Law—the *Bundestag* expressed that it does not consider such measures to interfere with Article 10. In other words, the *Bundestag* followed the line of argumentation of the Federal Government that foreigners abroad are not entitled to protection by this basic right. In the following part, this approach will be critically assessed.

C. The Constitutional Law Dimension of Strategic Surveillance by the BND

This part examines whether the law and practice of the BND in the field of strategic surveillance is in line with the German Basic Law. First, it will be highlighted to what extent the privacy of electronic communication is generally protected by the Basic Law. Then, it will be asked whether non-German nationals who are affected by strategic surveillance measures of the BND outside the territory of the Federal Republic of Germany are also entitled to such protection. This question might appear somewhat strange from a U.S. perspective as it is firmly established that the Fourth Amendment to the U.S. Constitution does not protect nonresident aliens in foreign countries against surveillance by the NSA.[140] The U.S. Supreme Court stated in *United States v. Verdugo-Urquidez* that the purpose of the

[140] For a parallel discussion under U.S. constitutional law, see Miller, *supra* note 32, at 90; Alec Walen, *Fourth Amendment Rights for Nonresident Aliens*, 16 GERMAN L.J. 1131 (2015). For a different perspective, see Asaf Lubin, *"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, 18 CHICAGO J. INT'L L. 502 (2018) (making the case for certain legal differentiations in treatment between domestic and foreign surveillance).

Fourth Amendment is to protect the people of the United States against arbitrary action by their own government and not to restrain the government's actions against aliens outside U.S. territory.[141] The NSA has therefore nearly unlimited authority to spy on foreign nationals while they are outside the United States.[142] Under German constitutional law, the issue of extraterritorial basic rights protection for foreigners leaves more room for discussion. Here, the answer depends on how the personal and territorial scope of Article 10 and other basic rights enshrined in the Basic Law is defined.

I. The Privacy of Electronic Communication Under German Constitutional Law

German constitutional law ensures the protection of privacy in various aspects. While the privacy of correspondence, posts, and telecommunications as well as the inviolability of the home are expressly guaranteed in the Basic Law (Articles 10 and 13), other privacy protections have been derived by the Federal Constitutional Court from the general right to personality, which flows from Article 2(1) of the Basic Law (personal freedoms) in conjunction with the human dignity clause contained in Article 1(1).

As far as the surveillance of electronic communication is concerned, the most relevant provision in the Basic Law is Article 10, establishing that the privacy of correspondence, posts, and telecommunications shall be inviolable.[143] This provision is interpreted by the Federal Constitutional Court in a rather dynamic fashion to cover the whole spectrum of digital communication, irrespective of the technology used and the content transmitted.[144] It also protects the confidentiality of the circumstances of the communication, which includes all kinds of metadata.[145] Whether the communication is intercepted *en route*, for example, at an Internet exchange point, or directly at the phone or computer used by the sender or recipient is irrelevant. Any monitoring and recording of an ongoing communication process as well as any screening, storage, transfer, or other processing or use of related communication data is considered an encroachment upon Article 10 and requires a specific legal basis in statutory law.[146]

---

[141] United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

[142] Cole & Fabbrini, *supra* note 33, at 228–33.

[143] For an overview, see Thomas Schwabenbauer, *Kommunikationsschutz durch Art. 10 GG im digitalen Zeitalter* [Protection of Communication by Article 10 GG in the Digital Age], 137 ARCHIV DES ÖFFENTLICHEN RECHTS [AÖR] 1 (2012) (Ger.).

[144] *See, e.g.*, Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 67 BVERFGE 157 (172); 100 BVERFGE 313 (358); 106 BVERFGE 28 (36); 113 BVERFGE 348 (383); 120 BVERFGE 274 (307) (Ger.).

[145] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 115 BVERFGE 166, (183) (Ger.).

[146] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 100 BVERFGE 313 (359, 366); 125 BVERFGE 260 (309) (Ger.).

The Federal Constitutional Court decided in a number of cases that the core area of private life, which is guaranteed by Article 1(1) of the Basic Law, must be respected under any circumstances.[147] As mentioned above, even the greater public good cannot justify interference with the core area of private life of an individual.[148] Part of the core area of private life are perceptions, feelings, considerations, views, and experiences of a highly personal character.[149] Notably, information that is directly linked to a criminal offense is exempt from such protection.[150] To ensure an adequate protection of the core area of private life, the intelligence authorities must observe certain procedural safeguards. Surveillance measures must be stopped if there is reasonable ground to believe that an act of surveillance will lead to information relating to the core area of private life. Should such information have been inadvertently recorded, it must be deleted immediately.[151]

Article 10 of the Basic Law, however, applies only to an ongoing communication process. Exempt from this protection is the confidentiality of data that relate to the content or circumstances of a completed communication and that are already stored in the sphere of the participants.[152] This means that a State agency which uses spying software to infiltrate and search the storage medium of a smartphone or computer of a suspected person via the Internet does not interfere with Article 10.[153] Therefore, the Federal Constitutional Court in the *Online Computer Surveillance Case* of 2008 derived from the general right to personality the so-called "right to the guarantee of the confidentiality and integrity of information technology systems" (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*).[154] The general right to personality had already served the Court several times as a basis for closing privacy protection gaps in light of new technological advancements. In the *Census Act Case* of 1983, for example, the Court developed the right to informational self-determination (*Recht auf informationelle Selbstbestimmung*).[155] Here, the Court held that, under modern conditions of data processing, the individual had to be

[147] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 34 BVERFGE 238 (245); 109 BVERFGE, 279 (313); 120 BVERFGE 274 (335–39) (Ger.).

[148] *See supra* note 67 and accompanying text.

[149] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 80 BVERFGE 367 (375) (Ger.).

[150] *Id.*

[151] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 113 BVERFGE 348 (391); 120 BVERFGE 274 (337) (Ger.).

[152] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 115 BVERFGE 166 (183) (Ger.).

[153] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 120 BVERFGE 274 (308) (Ger.).

[154] *Id.* For a summary of this case, see KOMMERS, *supra* note 52, at 417.

[155] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 65 BVERFGE 1 (Ger.). *See also* KOMMERS, *supra* note 52, at 408.

protected from unlimited collection, storage, use, and transmission of personal data.[156] Later, the Court expounded that the protective scope of the right to informational self-determination was not limited to information of an inherently sensitive character. In its view, even the handling of personal data that was less meaningful by itself could have serious repercussions on the privacy and freedom of action of the individual, depending on the purpose of the collection and the mode of processing.[157] In the *Online Computer Surveillance Case*, however, the Court came to the conclusion that the right to informational self-determination did not fully accommodate the new vulnerabilities and privacy risks resulting from the use of highly advanced and interconnected communication systems.[158] The use of such systems would inevitably lead to the creation, processing, and storage of large quantities of data. A third party accessing a system could therefore obtain data stocks that are extremely revealing. The severity of such an intrusion, as the Court noted, goes far beyond the quality of individual data collections against which the right to informational self-determination provides protection. To close this gap, the Court developed the right to the guarantee of the confidentiality and integrity of information technology systems. This right aims to protect the individual against State intrusions in systems that alone or in a network environment contain personal data to such an extent and in such diversity, that access to the system would enable the intruder to gain insight into significant parts of the life of a person and to generate detailed personality profiles.[159]

Every restriction of these basic rights requires a statutory basis. It is established under German constitutional law that all essential decisions concerning the implementation of a basic right—in particular decisions to interfere with the exercise of a basic right—must be taken by the parliament in the form of a statute (*Wesentlichkeitslehre, Parlamentsvorbehalt*).[160] This flows from the principle of the *Rechtsstaat*[161] (Article 20(3) of the Basic Law) and the democracy principle (Article 20(2)), which are cornerstones of the German constitution. Any statutory provision that restricts a basic right must be entirely in accordance with the Basic Law. In particular, it must serve a legitimate purpose and respect the principle of proportionality, which also follows from the principle of the *Rechtsstaat*.[162] Moreover, the occasion, purpose, and limits of the encroachment must be defined in a

[156] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 65 BVERFGE 1 (43) (Ger.).

[157] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 120 BVERFGE 378 (398) (Ger.).

[158] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 120 BVERFGE 274 (311–13) (Ger.).

[159] *Id.* at 303–14.

[160] *See, e.g.*, Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 49 BVERFGE 89 (126) (Ger.); 83 BVERFGE 130 (142) (Ger.).

[161] On the meaning of the term "*Rechtsstaat*," see KOMMERS, *supra* note 52, at 48.

[162] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 19 BVERFGE 342 (349) (Ger.).

sufficiently specific, precise, and clear manner.[163] This requirement is often referred to as the "principle of determinedness and clarity of legal norms" (*Gebot der Normenbestimmtheit und Normenklarheit*). The required level of determinedness and clarity depends on how significantly a basic right is affected. A provision summarizing the tasks of an agency, like Section 1(2)(1) of the BND Act, does not automatically authorize an encroachment upon basic rights in the fulfillment of these tasks. Furthermore, the law must apply generally and not merely to a single case (Article 19(1)(1) of the Basic Law); it must expressly specify the affected basic right and the relevant Article (Article 19(1)(2)), and the essential content of the affected basic right must not be impaired (Article 19(2)).

In the *G10 Act Case* of 1999, the Federal Constitutional Court spelled out detailed parameters for regulating strategic surveillance.[164] These parameters have been translated by the German legislator into the 2001 version of the G10 Act. The outer boundaries for an admissible surveillance legislation were explored by the Federal Constitutional Court in a judgment of 2010 dealing with the issue of data retention.[165] In this judgment, the Court stated that legislation which would aim at storing personal data in a precautionary way and as comprehensively as possible for the purpose of future criminal prosecution or threat prevention would be per se incompatible with the German constitution.[166] Moreover, the Court made clear that it is part of the constitutional identity of the Federal Republic of Germany that the citizens, in the exercise of their individual freedoms, must not be subject to total surveillance.[167]

II. Are Non-German Nationals in Foreign Countries Protected by Article 10 of the Basic Law?

The German Basic Law generally distinguishes between two types of basic rights: Those which afford protection to every human being and those which explicitly apply to German nationals only (*Deutschengrundrechte*).[168] Neither Article 10 nor the rights derived from Article 2(1) and Article 1(1) are limited in their application to German nationals. This means that, at least within German territory, all individuals, irrespective of their nationality, are

[163] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 65 BVERFGE 1 (46); 100 BVERFGE 313 (360); 110 BVERFGE 33 (53); 113 BVERFGE 348 (375); 120 BVERFGE 274 (316); 120 BVERFGE 378 (407) (Ger.).

[164] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 100 BVERFGE 313 (359–62) (Ger.).

[165] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 125 BVERFGE 260 (323) (Ger.).

[166] *Id.*

[167] *Id.* at 324.

[168] Basic rights that apply only to German nationals include, e.g., the freedom of assembly (Article 8 of the Basic Law), the freedom of association (Article 9), and the freedom of movement (Article 11). With regard to the exercise of such freedoms, foreigners enjoy basic protection under Article 2(1), which guarantees a general freedom of action for every person.

protected. It is not required that the person is a lawful resident of Germany. Any discrimination in this regard would also violate Article 3(1) of the Basic Law (equality before the law).

A different question is: Does the Basic Law protect foreign nationals who are affected by the actions of German authorities outside the territory of the Federal Republic of Germany—and, if so, is the standard of protection the same as if the affected persons had been within Germany? The Federal Constitutional Court has not yet taken a stance on this particular issue. In the *G10 Act Case* of 1999, it only made general remarks on the geographical dimension of the protective scope of Article 10.[169] In this case, the Federal Government argued that German authorities were not bound to apply the basic rights everywhere in the world and under any circumstances.[170] According to the Government, the effects resulting from the exercise of State authority abroad would trigger basic rights protection only to the extent that such effects were based on the personal or territorial jurisdiction of Germany.[171] A German national who leaves the Federal Republic of Germany is still subject to Germany's personal jurisdiction and therefore remains protected by the basic rights vis-à-vis the German State. What the Federal Government meant by arguing that an exercise of authority could trigger basic rights protection to the extent that it was based on territorial jurisdiction is less clear. In the view of the Government, there had to be a link between the act in question and the territory of the Federal Republic of Germany.[172] The Federal Constitutional Court left it deliberately open whether there really must be a territorial link. The Court only stated that, whenever the BND used installations on German soil to intercept and record telecommunication, there would be such a link.[173] Moreover, the Court noted that the process of analyzing these communications, which also constitutes an encroachment upon Article 10 of the Basic Law, would usually take place on German territory.[174] In these constellations, where there was an evident nexus between surveillance activities that were technically conducted from within Germany and the target of such activities located abroad (*technisch-informationelle Beziehung*), the BND would be bound by Article 10.[175] At the same time, the Court straightened out that its remarks on the territorial reach of Article 10 did not

[169] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 100 BVERFGE 313 (362–64) (Ger.).

[170] *Id.* at (338–39) (summarizing the position of the Federal Government).

[171] *Id.* at 339.

[172] *Id.*

[173] *Id.* at 363.

[174] *Id.*

[175] *Id.* at 363–64.

concern the specific question of whether Article 10 also protected foreign nationals abroad.[176]

The starting point for approaching this issue is Article 1(3) of the Basic Law, which stipulates that the basic rights bind the German legislature, the executive, and the judiciary as directly applicable law. It means that no organ of the State may perform its sovereign functions without respecting the restrictions imposed by these rights. Article 1(3) does not contain any language that would imply a territorial limitation of the binding force of the basic rights. In 1957, the Federal Constitutional Court already made clear that German State organs are bound by the basic rights even in cases in which the effects of the exercise of authority occur abroad.[177] Hence, it is generally acknowledged that all three branches of the State remain bound by the basic rights when they exert their powers outside German territory.[178] This understanding adequately reflects the realities of a globalized world in which "traditional borders have become permeable" and "State organs operate more frequently and more intensely outside the domestic territory."[179]

Article 1(3) of the Basic Law, however, defines the reach of the basic rights' binding force only in general terms. Therefore, "each specific basic right has to be defined *ratione loci*, *ratione materiae*, and *ratione personae*."[180] The next step is thus to find out whether Article 10 of the Basic Law is open for an application in transnational constellations. Like Article 1(3), Article 10 does not contain any language that would restrict its application to the territory of the Federal Republic of Germany. It is an "impact-related" right that serves to protect the individual against intrusive actions by the State wherever such actions occur. As noted above, the Federal Constitutional Court has always interpreted Article 10 in a rather dynamic fashion to cover the whole spectrum of digital communication. Given the fact that digital communication is of paramount importance for the free exchange of opinions and

---

[176] *Id.* at 364.

[177] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 6 BVERFGE 290 (295). *See also* 57 BVERFGE 9 (23) (Ger.).

[178] Matthias Herdegen, *Art. 1 Abs. 3*, *in* MAUNZ/DÜRIG GRUNDGESETZ KOMMENTAR n. 71 (Roman Herzog, Matthias Herdegen, Hans H. Klein & Rupert Scholz eds., 2016); Christian Hillgruber, *Art. 1*, *in* BECK'SCHER ONLINE-KOMMENTAR GG n. 76 (Volker Epping & Christian Hillgruber eds., 26th ed. 2015); Hans D. Jarass, *Art. 1*, *in* GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND 37, 52 (Hans D. Jarass & Bodo Pieroth eds., 10th ed. 2009); BODO PIEROTH, BERNHARD SCHLINK, THORSTEN KINGREEN & RALF POSCHER, GRUNDRECHTE—STAATSRECHT II 55 (31st ed. 2015); Martin Heidebach, *Die NSA-Affäre in Deutschland—Stößt der Grundrechtsschutz an seine Grenzen?* [*The NSA Affair in Germany—Does Basic Rights Protection Reach Its Limits?*], 68 Die Öffentliche Verwaltung [DÖV] 593 (2015); HEIKE KRIEGER, DIE REICHWEITE DER GRUNDRECHTSBINDUNG BEI NACHRICHTENDIENSTLICHEM HANDELN [THE REACH OF THE BINDING CHARACTER OF THE BASIC RIGHTS IN THE CASE OF INTELLIGENCE ACTIVITIES] 3–6 (2008), http://www.jura.fu-berlin.de/fachbereich/-einrichtungen/oeffentliches-recht/lehrende/kriegerh/dokumente/berliner_online_beitraege_krieger08_01.pdf.

[179] Gärditz, *Legal Restraints*, *supra* note 30, at 408.

[180] *Id.* at 409.

information between people across the globe, it is difficult to see why the privacy of such communication should not be subject to protection by Article 10 in constellations of a transnational character.

Because Article 10 of the Basic Law functions as a protective right against the State, its application is triggered only if there is an exercise of State authority. At this point, it may be useful to draw a distinction between two types of action: (1) the collection of intelligence *on foreign territory*; and (2) the collection of signals intelligence about foreign countries and their citizens *with installations located on German territory*. As far as clandestine activities by agents on foreign soil are concerned, it has been claimed that the deployed agents did not exercise sovereign authority.[181] The main argument is that the conduct of an organ of the executive branch would constitute an exercise of State authority only if the organ was in fact able to exert some form of sovereign control and had the power to enforce its decisions, if necessary, by means of legal coercion.[182] This view resorts to the "effective control" test developed by the European Court of Human Rights.[183] The European Court of Human Rights has taken the position that there must be exceptional circumstances to justify an extraterritorial application of the rights and freedoms enshrined in the European Convention on Human Rights (State agent authority and control; or effective control over an area).[184] Referring to that test, it is held that "[c]landestine intelligence gathering abroad cannot be qualified as an 'exceptional circumstance' that would establish *de facto* effective control."[185] In the logic of this argument, the activities of the BND abroad are not a manifestation of sovereign power. Instead, the agents would act like a private person in the sphere of illegality. At best, they had "the merely factual power of a gang of criminals."[186] Assessing the plausibility of this argument is beyond the scope of the present Article. It may help to explain, though, why the German legislator has so far abstained from regulating

[181] *Id.* at 409–15.

[182] Gärditz, *Rechtsbindung*, *supra* note 31, at 474.

[183] Gärditz, *Legal Restraints*, *supra* note 30, at 410–11.

[184] The *Al-Skeini Judgment* of 2011 provides an overview of the relevant jurisprudence on these matters. *See* Al-Skeini and Others v. The United Kingdom, App. No. 55721/07, paras. 130–142 (July 7, 2011).

[185] Gärditz, *Legal Restraints*, *supra* note 30, at 411.

[186] *Id.* at 412.

intelligence collection by the BND on foreign territory.[187] As far as such activities are concerned, the BND still operates on the basis of Section 1(2)(1) of the BND Act.[188]

More relevant from the perspective of this Article is the second type of action: The surveillance of communications that involve foreign nationals in foreign countries—but with installations located within Germany's territorial jurisdiction. In these cases, there is no doubt that the BND exercises State authority by implementing the provisions contained in the G10 Act and the BND Act. The very purpose of these laws is to regulate such transboundary surveillance operations. This means that the BND is automatically bound by Article 10 of the Basic Law irrespective of the nationality and location of the affected persons.[189] With a view to such constellations, two important features of basic rights protection must be considered in combination: Article 10 protects every natural person without regard to nationality, and it is applicable in situations in which the effects of an exercise of State authority occur abroad. This position is shared by the vast majority of German constitutional lawyers.[190] Even the U.N. Special Rapporteur on the Right to Privacy has recently criticized the German legislation in an unusually harsh manner.[191] In his view, the new BND law "loses out on a precious opportunity to clarify that the right to privacy and related safeguards applies to individuals irrespective of nationality, citizenship or location, or indeed whether the surveillance is carried out inside or outside Germany."[192] The question of whether foreigners "deserve" privacy protection has also been the subject of some discussion under international human rights law. In this debate, it has been maintained that "it is difficult to see how citizenship serves as a legitimate distinction with regard to

[187] While States are generally prevented by international law from exercising their authority and enforcing their laws on the territory of other States (unless they are specifically entitled to do so), they are not prevented from enacting legislation that defines for their own agencies the scope and parameters for intelligence operations abroad. Theoretically, the German legislator could therefore also adopt provisions regulating the BND's engagement in such operations, which would further enhance legal certainty.

[188] *Supra* note 81.

[189] *But see* Gärditz, *Legal Restraints*, *supra* note 30, at 419 (doubting that the qualitative threshold for triggering protection by Article 10 of the Basic Law is reached when a measure of strategic surveillance merely scans metadata to reveal potential patterns without individualizing the participants).

[190] *See, e.g.*, Manfred Baldus, *Art. 10*, *in* BECK'SCHER ONLINE-KOMMENTAR GG n. 21 (Volker Epping & Christian Hillgruber eds., 26th ed. 2015); Wolfgang Durner, *Art. 10*, *in* MAUNZ/DÜRIG GRUNDGESETZ KOMMENTAR n. 64 (Roman Herzog, Matthias Herdegen, Hans H. Klein & Rupert Scholz eds., 2016); Jarass, *supra* note 178, at 52; PIEROTH, *supra* note 178, at 37; Bäcker, *supra* note 31, at 561; Hölscheidt, *supra* note 31, at 153; Marxsen, *supra* note 31, at 225–27; Mehrdad Payandeh, *Entterritorialisierung des Öffentlichen Rechts: Transnationale Individualrechtsverletzungen zwischen Verfassungsrecht und Völkerrecht* [*Deterritorialization of Public Law: Transnational Violations of Individual Rights Between Constitutional Law and International Law*], 131 DEUTSCHES VERWALTUNGSABLATT [DVBL] 1073, 1076–77 (2016); KRIEGER, *supra* note 178, at 3–10. For further references, see Papier, *supra* note 31, at 3.

[191] Report of the Special Rapporteur on the Right to Privacy, 21, U.N. Doc. A /71/368 (Aug. 30, 2016).

[192] *Id.*

surveillance and communications privacy secured by Article 17 [of the European Convention on Human Rights]."[193] Another commentator noted that "under the moral logic of human rights law, citizens and non-citizens are equally deserving of protection of their rights generally, and privacy specifically."[194]

Insofar as it is acknowledged that Article 10 of the Basic Law also protects foreigners abroad, the issue nevertheless remains as to whether the standard of protection is the same as the standard that applies in Germany. The Federal Constitutional Court pointed out that the reach and level of protection guaranteed by the basic rights in an international context is open to certain differentiations and modifications.[195] This may be the case if the complete implementation of a basic right on foreign territory would conflict with Germany's international obligations or if Germany would be factually prevented from fully enforcing its own basic rights standards abroad. The Federal Constitutional Court clarified that the protective scope of the basic rights ends where another State is alone responsible for a certain development.[196] If it is to be expected that an applicable basic right might become completely sidelined and irrelevant in an international context, the German legislator may choose to lower the standards regarding the implementation of that right in order to preserve at least some degree of protection.[197] The realities of international relations and the need for international cooperation sometimes call for such compromises. But transnational constellations do not per se warrant a lowering of the standards of basic rights protection. Any differentiation or modification must be justified in light of the specific circumstances of the case at hand.[198]

In the present context it is doubtful, for example, whether the provisions of the G10 Act concerning the notification of affected persons could or should be applied in situations in which the affected person is a foreign national not living in Germany.[199] A strict

[193] Peters, *supra* note 14, at 163.

[194] Milanovic, *supra* note 14, at 100.

[195] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 31 BVERFGE 58 (75–77); 100 BVERFGE 313 (363) (Ger.). *See also* Herdegen, *supra* note 178, n. 72; RAINER HOFMANN, GRUNDRECHTE UND GRENZÜBERSCHREITENDE SACHVERHALTE 30–73 (1994).

[196] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 66 BVERFGE 39 (62) (Ger.). *See also* Herdegen, *supra* note 178, n. 75.

[197] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 92 BVERFGE 26 (41–42) (Ger.).

[198] Payandeh, *supra* note 190, at 1076, 1080.

[199] Matthias Bäcker, Stellungnahme zu dem Entwurf eines Gesetzes zur Ausland-Ausland–Fernmeldeaufklärung des Bundesnachrichtendienstes [Statement Regarding the Draft Act on the Collection of Foreign-Foreign Communications Intelligence by the Federal Intelligence Service], DEUTSCHER BUNDESTAG, INNENAUSSCHUSS: AUSSCHUSSDRUCKSACHE 18(4)653 G, Sept. 23, 2016, at 10, https://www.bundestag.de/blob/459630/1ddfe2451c0fd067872976d0f0467882/18-4-653-g-data.pdf (Ger.)

implementation of these provisions in a transnational context would force the BND to disclose to some extent its activities vis-à-vis the State in which the person is present. This could have severe operational consequences for the BND.[200] Apart from that, a formal notification may require administrative measures on the territory of the relevant State, which could raise additional problems in terms of cooperation. In certain cases, the target person might even be exposed to grave harm in his or her home country if the local authorities were informed and involved in the process. It is not excluded that other protections contained in the G10 Act are also open for certain modifications, but it would be difficult to argue that the entire regime on *Ausland-Ausland-Fernmeldeaufklärung* in the BND Act is per se an admissible modification of the G10 regime.

III. The Privacy of Electronic Communication of Companies, NGOs, and Other Legal Persons in a Transnational Context

Article 19(3) of the Basic Law determines that the basic rights shall apply to domestic legal persons as far as the nature of the right permits such application. Basic rights are first and foremost protective rights against the State.[201] Therefore, the Federal Constitutional Court acknowledged that the basic rights are applicable to a legal person that is organized under public law only insofar as the entity serves the free development of the individuals who stand behind it.[202] This exception applies mainly to churches, universities, and public broadcasting stations.

The reference to *domestic* legal persons in Article 19(3) of the Basic Law makes clear that the basic rights do not protect foreign legal persons. The distinction between domestic and foreign legal persons refers to the location from where the entity is effectively operated. If a company is registered and has its headquarters in Germany, it is usually assumed that the company is a domestic legal person, even if owned or managed by foreigners.[203] In the case of multinational corporations and their subsidiaries, the distinction may prove more difficult.

Private legal persons that have their hub in another EU Member State are accorded a special status under German constitutional law. The Federal Constitutional Court decided that such entities shall benefit from an extension of the scope of application of the German basic

---

[hereinafter Bäcker, Statement Innenausschuss] (discussing the requirements of Article 10 of the Basic Law in the context of the collection of signals intelligence regarding foreign nationals abroad); KRIEGER, *supra* note 178, at 10.

[200] Dietrich, *supra* note 36, at 414.

[201] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 21 BVERFGE 362 (369) (Ger.).

[202] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 61 BVerfGE 82 (102) (Ger.).

[203] Hans D. Jarass, *Art. 19*, *in* GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND 446, 456 (Hans D. Jarass & Bodo Pieroth eds., 10th ed. 2009).

rights.[204] According to the Court, such an extension is required because of the primacy of the freedoms of the internal market as enshrined in Article 26(2) of the Treaty on the Functioning of the European Union (TFEU) and because of the general prohibition on discrimination laid down in Article 18 TFEU.[205] This means that Article 19(3) of the Basic Law must be interpreted in a way that does not exclude EU private legal persons from basic rights protection when they operate "within the scope of application of the Treaties."[206] Companies that depend on the free movement of goods, persons, services, and capital within the EU can invoke non-discrimination provisions of EU law. It may thus be argued that the BND is under an obligation to treat the communication of such companies as G10 communication, subject to the same protection as communications of domestic legal persons.[207]

Foreign State and governmental authorities, however, are under no circumstances covered by the protective scope of the German basic rights (for the same reasons as German legal persons that are organized under public law are generally prevented from invoking protection). Hence, it is firmly established that espionage directed against foreign authorities and public officials, while acting in their official capacity, is not a case where Article 10 of the Basic Law would be applicable.[208] Such persons are protected only as far as their individual privacy sphere is affected.[209]

An interesting issue, which has come up during the hearings before the Committee of Inquiry of the *Bundestag*, was the BND's interpretation of the protective scope of Article 10 of the Basic Law in cases in which a German national works for a foreign company, NGO, or other foreign institution abroad. According to the so-called *Funktionsträger* theory developed by the BND, German nationals could not claim that their communication was protected by Article 10 of the Basic Law as long as they communicated in their capacity as a representative of such a company, NGO, or institution outside the territory of the Federal Republic of Germany.[210] The BND treats such communication as routine communication and not as G10

[204] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 129 BVerfGE 78 (94) (Ger.).

[205] *Id.*

[206] Consolidated Version of the Treaty on the Functioning of the European Union art. 18(1), Oct. 26, 2012, 2012 O.J. (C 326) 47 ("Within the scope of application of the Treaties, and without prejudice to any special provisions contained therein, any discrimination on grounds of nationality shall be prohibited.").

[207] Huber, *supra* note 50, at 1402; Bäcker, Statement Innenausschuss, *supra* note 199, at 11.

[208] Papier, *supra* note 31, at 5.

[209] Gärditz, *Rechtsbindung*, *supra* note 31, at 478.

[210] *See* Graulich Report, *supra* note 60, at 44 (summarizing the BND's *Funktionsträger* theory); Notification by the Parliamentary Control Panel, *supra* note 7, at 5 (pointing to the controversial character of the *Funktionsträger*

communication. Vice versa, in the logic of this theory, a foreign national would benefit from basic rights protection if he or she worked for a German company or NGO abroad. It means, for example, that an Afghan national employed by a German NGO in Afghanistan—while acting in his capacity as a representative of that company—would be protected by Article 10, whereas a German employee of a Canadian company in Afghanistan acting in such capacity would not enjoy protection. But this theory can hardly be brought in line with basic rights doctrine. According to the Federal Constitutional Court, Article 10 does not differentiate between the private, business, or political content of a communication.[211] The participants of a communication do not lose privacy protection just by using a corporate phone or computer.[212] In the view of the present author, the *Funktionsträger* theory has no basis in German constitutional law, irrespective of whether German nationals or foreigners abroad are concerned.

D. Concluding Remarks: A Reality Check

In part B, it has been demonstrated that German intelligence law distinguishes between certain categories of communications depending on the nationality and location of the participants. The provisions on the surveillance of foreigners abroad are far more permissive than those applying to the monitoring of communications that involve German nationals or foreigners in Germany. This differentiation is the consequence of a narrow interpretation of the personal and territorial scope of Article 10 of the Basic Law. It is an established principle that German nationals enjoy protection under Article 10 wherever their privacy is affected by the actions of the German State. Foreigners, however, are considered by the German legislator, the Federal Government, and the BND to be entitled to such protection only while staying in Germany. In part C, it has been argued that such differentiation is difficult to reconcile with German constitutional law because Article 10 protects every natural person without regard to nationality and because the Article's scope of application is not limited to the territory of the Federal Republic of Germany. It is therefore important to stress that the BND is bound by Article 10 irrespective of whether its surveillance activities affect German nationals, foreigners in Germany, or foreigners abroad. If basic rights protection is taken seriously, the G10 Act and the BND Act must be revised accordingly. The existing fragmented legislation should have been subject to a reform more comprehensive than the 2016 amendment of the BND Act. A more viable alternative would be a uniform statutory regime

theory). *See also* Report of the 1st Committee of Inquiry, *supra* note 3, at 710–13 (quoting from an internal handbook of the BND).

[211] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] 67 BVERFGE 157 (172); 100 BVERFGE 313 (358); 106 BVERFGE 28 (36) (Ger.).

[212] Matthias Bäcker, *Der BND baut sich einen rechtsfreien Raum: Erkenntnisse aus dem NSA-Untersuchungsausschuss* [*The BND Is Creating a Legal Vacuum: Insights from the NSA Committee of Inquiry*], VERFASSUNGSBLOG (Jan. 19, 2015), http://verfassungsblog.de/der-bnd-baut-sich-einen-rechtsfreien-raum-erkenntnisse-aus-dem-nsa-untersuchungsausschuss/.

for strategic surveillance of international communications that meets the minimum requirements of Article 10 (perhaps not necessarily the high standards contained in the G10 Act) without bearing reference to a person's nationality or location. Of course, it would be a difficult challenge for lawmakers to strike a balance between the requirements dictated by Article 10 in transnational constellations and the need for operational flexibility, especially with a view to international intelligence cooperation. Sooner or later, the Federal Constitutional Court will have to deal with these issues in greater detail. The current state of law has been described as follows: "Legal doctrine is embryonic. The scarce and scattered cases that actually depended on basic rights protection abroad do not provide a coherent jurisprudence. The German Federal Constitutional Court is still meandering through these issues, following a 'muddling through' approach that has not provided stable and predictable parameters for the parliament."[213]

But German intelligence legislation is not only problematic from a constitutional law perspective. It is also predicated on the unrealistic assumption that separating domestic communications from foreign communications and identifying the nationality and location of each participant is technically feasible.[214] In the age of the Internet, it is practically impossible to maintain such a strict separation between different types of communication. First of all, it is difficult to predict on which route a particular communication will be transmitted. In the past, electronic communication was transmitted through direct lines, which were connected by operators (circuit switching). This means that the entire communication between the participants ran through one and the same standing line. In the age of circuit switching, it was possible to identify certain cables channeling communication exclusively between two countries or regions. Some key provisions of the G10 Act are specifically designed to apply under such conditions.[215] Today, however, electronic communication data are mostly transmitted as addressed packets in fiber optic cables. For that purpose, a communication is split into several smaller packets that may be transported on completely different routes and put together at the end of the travel before they reach the phone or computer of the recipient (packet switching). These packets will usually not take the most direct path. According to experts, it is not possible anymore, under the conditions of packet switching, to distinguish easily between purely domestic communication traffic and international traffic.[216] Due to the complexity of the structure of

[213] Gärditz, *Legal Restraints*, *supra* note 30, at 431.

[214] *See also* Marxsen, *supra* note 31, at 227.

[215] *See* G10 Act § 10(4) (requiring that only a certain portion of the transmission capacity of a particular transmission channel may be subject to surveillance and that this portion must be determined before the measure starts).

[216] Kay Rechthien, Frank Rieger & Constanze Kurz, Sachverständigengutachten gemäß Beweisbeschluss SV-13 [Expert Opinion According to Evidence Order SV-13], 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages [1st Committee of Inquiry of the 18th legislative period of the German Bundestag], Sept. 30, 2016, at 2, https://www.ccc.de/system/uploads/220/original/beweisbeschluss-nsaua-ccc.pdf (describing the technical conditions applying to packet switched transmission of telecommunication data). *See also* Gabi Dreo

the Internet and due to other factors that characterize the ad hoc and highly dynamic character of packet switching (such as the variety of different service models, complex decisions concerning the allocation and utilization of network capacity, rapid changes in routing patterns, etc.), it is hard to predict which data packets will be transported on a certain line between two routers.[217]

Moreover, it is questionable whether the BND is really able to separate, with the necessary degree of reliability, purely domestic communications, G10 communications, routine communications, and communications with an EU background—which are all subject to different levels of protection against surveillance under current intelligence law. The BND uses special filter systems to screen communication streams in various cascades until all communications of a certain category are singled out.[218] At an early stage of this process, communications are to be identified on the basis of general technical parameters (country codes relating to telephone numbers, e-mail addresses, country code top-level domains, etc.). Moreover, the filters automatically run through lists containing identifiers that relate to communication infrastructure used by legal persons and individuals already known to the BND (e.g. "G10 lists" of German company offices in foreign countries). It has been reported, however, that these filter systems are not as sophisticated as to provide reliable results in all cases.[219] To verify that a particular selector (e.g. a telephone number or e-mail address) or an intercepted communication is linked to a German company, an EU institution, or an authority of an EU Member State may be relatively easy. Clarifying whether an individual participant is a German national, a foreign EU citizen, or a non-EU foreigner, however, poses considerable practical problems. Does the use of a Belgian e-mail address, for instance, provide sufficient evidence for the assumption that the participant located in Afghanistan is

---

Rodosek, Sachverständigengutachten gemäß Beweisbeschluss SV-13 [Expert Opinion According to Evidence Order SV-13], 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages [1st Committee of Inquiry of the 18th legislative period of the German Bundestag], Sept. 30, 2016, at 19–23, https://cdn.netzpolitik.org/wp-upload/2016/10/gutachten_ip_lokalisation_rodosek.pdf.

[217] Rechthien, Rieger & Kurz, *supra* note 216, at 6. *See also* Michael Waidner, Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 26. Juni 2014 [Statement on Hearing by the Committe of Inquiry], Deutscher Bundestag, 1. Untersuchungsausschuss der 18. Wahlperiode [1st Committee of Inquiry of the 18th Legislative Period], Doc. MAT A SV-1/2 on A-Drs. 53, June 26, 2014, at 11 (describing the basic parameters for communication on the Internet).

[218] *See, e.g.*, Antwort der Bundesregierung [Response by the Federal Government], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 17/14739, at 14 (Ger.) (noting that purely domestic (German) communications are neither captured nor stored in the course of a strategic surveillance measure under Section 5(1) of the G10 Act); Gesetzesentwurf der Fraktionen der CDU/CSU und SPD [Draft Act by the Parliamentary Groups CDU/CSU and SPD], DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/9041, at 24 (Ger.) (describing the use of filters for the purpose of sorting out protected G10 communications in the course of *Ausland-Ausland-Fernmeldeaufklärung* under the BND Act); Graulich Report, *supra* note 60, at 27–30 (describing in greater detail the filtering process relating to the use of selectors).

[219] Mascolo, Leyendecker & Goetz, *supra* note 5. *See also* Report of the 1st Committee of Inquiry, *supra* note 3, at 1444–51.

in fact a Belgian national? And what happens if a Belgian uses a cellphone with an Afghan number? Even translators and intelligence analysts who would listen to an overseas telephone conversation and who may be well trained in recognizing local dialects may not be able to identify the nationality of the participants.

The problem is obvious: The G10 Act and the BND Act oblige the BND to make certain distinctions that apparently cannot be made with the necessary degree of reliability. In light of these realities, it would be advisable to reconsider whether the established categories in German intelligence law are still adequate. Doubts have also arisen from another angle: The U.N. Special Rapporteur on the Right to Privacy raised an important issue, alluding to the fact that the majority of the terrorist attacks carried out in Europe during the past two years was carried out by EU citizens, most often by the attacked states' own citizens.[220] One commentator appropriately summarized the issue with the following words: "In the counterterrorism and surveillance context, non-citizens neither inherently pose a greater threat to a state's security than its citizens, nor is their private information of inherently greater value or interest to the state."[221] The true value of surveillance laws that discriminate persons based on their nationality and location is therefore indeed difficult to see.

[220] Report of the Special Rapporteur on the Right to Privacy, *supra* note 191, at 20.

[221] Milanovic, *supra* note 14, at 101.