الأمم المتحدة

A/HRC/46/37/Add.3

الجمعية العامة

Distr.: General
8 July 2022
Arabic
Original: English

مجلس حقوق الإنسان

الدورة السادسة والأربعون

22 شباط/فبراير – 19 آذار/مارس 2021

البند 3 من جدول الأعمال

تعزيز وحماية جميع حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية

زيارة إلى ألمانيا

تقرير المقرر الخاص المعني بالحق في الخصوصية، جوزيف أ. كاناتاتشي* ** ***

موجز

قام المقرر الخاص المعني بالحق في الخصوصية، البروفيسور جوزيف أ. كاناتاتشي، بزيارة رسمية إلى جمهورية ألمانيا الاتحادية في الفترة من 29 تشرين الأول/أكتوبر إلى 10 تشرين الثاني/نوفمبر 2018. ويشير بارتياح إلى أن ألمانيا تحتفظ، بفضل ما يقرب من أربعين عاماً من القرارات المتسقة التي أصدرتها محكمتها الدستورية، بالمرتبة الأولى من بين 193 دولة عضواً في الأمم المتحدة في مجالين رئيسيين على الأقل لحماية الخصوصية. ويشملان الحماية الصريحة التي توفرها للخصوصية كجزء من دورها المتأصل في النماء الحر من دون عوائق للشخصية والمثال الذي تضربه لبقية العالم، حيث يمنح غير الألمان حماية الخصوصية نفسها حتى في سياق أنشطة الاستخبارات الأجنبية. ويثني المقرر الخاص على بعض الجهود التي تبذلها الحكومة الاتحادية الألمانية التي تحاول إدخال تحسينات هامة على ضمانات الخصوصية، ولكنه يوصي بقوة بمواصلة إصلاح القانون والآليات على نطاق واسع في الوقت نفسه لإدخال ضمانات جديدة وكذا زيادة فعالية سلطات الرقابة القائمة و/أو الجديدة.

* تصدر هذه الوثيقة من دون تحرير رسمي.

** يعمم موجز التقرير بجميع اللغات الرسمية. أما التقرير نفسه، المرفق بهذا الموجز، فيُعمم باللغة التي قُدّم بها فقط.

*** قُدم هذا التقرير بعد الأجل المحدد حتى يتضمن أحدث التطورات.

Annex

Report of the Special Rapporteur on the right to privacy on his mission to the Federal Republic of Germany

I. Introduction

A. Starting off

1. This report was finalised in spring 2021 after evaluating the preliminary results of the country visit as emerging from meetings held during the period on-site in the Federal Republic of Germany (BRD) from 29 October to 10 November 2018 and cross-checking these with follow-up research and developments to date. The benchmarks used for this report include the privacy metrics document released by the UN Special Rapporteur for Privacy, Professor Joseph A. Cannataci ("the Special Rapporteur").[1]

2. Some of the content of this report reflects and builds upon findings already published in the end-of-mission statement published in November2018 [2] as further validated to 12 April 2021. It also contains important up-dates gathered during close monitoring of the situation in the BRD since November 2018.

B. Acknowledgement and thanks

3. The Special Rapporteur thanks the German Federal and State Governments for the open way in which they greeted him and facilitated his visits. Discussions with Government officials were held in a cordial, candid and productive atmosphere.

4. The Special Rapporteur likewise thanks Civil Society, members of the Law Enforcement and intelligence communities, governmental officials and other stakeholders who presented him with detailed documentation and organised several meetings with him in order to provide detailed briefings.

5. The Special Rapporteur thanks those members of the German Federal and State Governments, and their staff who met with him and answered several questions, providing insights into issues of primary concern regarding privacy.

II. Constitutional and other legal protections of privacy

6. Germany's constitutional law regarding privacy is one which has relied far more extensively on the interpretations given by the German Federal Constitutional Court (*Bundesverfassungsgerich*t often abbreviated to BVerfG) rather than on any elaborate wording which explicitly protects privacy which may be found inside the 1949 *Grundgesetz* which today still serves as the country's written constitution.

---

[1] See. 'Metrics for Privacy -A Starting Point', Professor Joseph A. Cannataci https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex4_Metrics_for_Privacy.pdf This document was developed during the period 2017-2019 in order to enable the UN Special Rapporteur on the right to Privacy to maximise the number of common standards primarily concerning surveillance, against which a country's performance could be measured. It was refined at various stages and then changed its status from an internal checklist to a document released for public consultation in March 2019.

[2] Statement to the media by the United Nations Special Rapporteur on the right to privacy, on the conclusion of his official visit to Germany, 29 October to 9 November, issued on 9 November 2018. https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23854&LangID=E. The end of mission statement and this report should be read together, especially since, for reasons of available space and editing, some observations, available in the 2018 text, may have been omitted from this version of the report.

7. In this respect, it is worth pointing out the historical context, much of it linked to the development of UN human rights work, which should serve as a timely reminder of how international legal thinking about privacy is inextricably interwoven, while forming the crucible for Germany's invaluable contribution to the development of the overarching right to free development of personality:

(a) The American Declaration of the Rights and Duties of Man (ADRDM) of 2 May 1948 is the first international legal instrument to explicitly deal with the notion of free or unhindered development of personality. In Article XXIX. one reads "It is the duty of the individual so to conduct himself in relation to others that each and every one may fully form and develop his personality". The European Convention on Human Rights (ECHR) makes no mention of personality, a lacuna which is yet to be adequately remedied in treaty language at the pan-European level. This right is also explicitly recognised in Article 22 of the Universal Declaration of Human Rights (UDHR) which followed within 6 months in December 1948: "Everyone …is entitled to the realisation …of the rights indispensable for one's dignity and the free development of their personality." Article 29 UDHR also protects the right to develop one's personality: "[e]veryone has duties to the community in which alone the free and full development of his personality is possible."

(b) The ADRDM is also the first international legal instrument to explicitly embrace the right to dignity. Not only does dignity feature prominently in its preamble but it then features also when the right to property is presented as being additionally an enabling right to dimensions of privacy: Article XXIII. Every person has a right to own such private property as meets the essential needs of decent living and helps to maintain the dignity of the individual and of the home." Dignity of the home is an extremely interesting concept linked to the inviolability of private spaces and recurs frequently, if not necessarily always explicitly, in privacy studies and jurisprudence. Dignity is not explicitly mentioned in the European Convention on Human Rights but it features most prominently in the Charter of Fundamental Rights of the European Union (CFREU) which in 2000 established in its very opening article that "Human dignity is inviolable. It must be respected and protected." This is clearly a relatively late European attempt to partially remedy the silence of the ECHR about dignity and reflect the trend of a favourable approach to dignity within the jurisprudence of the European Court of Human Rights (ECtHR).

(c) These developments and differences about privacy-related concepts like dignity become even more interesting when examining another source of international law, the American Charter of Human Rights (ACHR) which came into existence in 1969 in order to give binding force to the ADRDM of 1948. The ACHR, under the title of Right to Privacy, has telescoped the 1948 separate provisions of the 1948 Bogota' ADHR into one provision very similar to the composite approach of Article 8 ECHR and Article 17 ICCPR: "No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence," Yet, under the same title "The Right to Privacy" the ACHR also bundles "honor" and "dignity" in its opening sub-Article 1 "Everyone has the right to have his honor respected and his dignity recognized." As will be seen below, bundling together dignity, honor and private life is something which would sometimes happen conceptually in Europe at the national level as opposed to pan-European legal texts.

(d) Article 11 ACHR takes a cue from the UN 1948 and 1966 texts and bundles honour and dignity in the same article as private life, indeed at the end of the same sentence identifying "the four interests", protecting them at the end of sub-article 2 from "unlawful attacks on his honor or reputation." This in contrast to the ECHR which only mentions reputation once, as something which is worth protecting in relation to the right of freedom of expression in Article 10.

(e) Article 11 ACHR is thus a very interesting, and to an extent, a very representative legal articulation of the conceptualisation of privacy. It paints a picture where a number of things come together to create a sphere of intimate human activity which is worthy of significant protection: a person's privacy and those places where it is most clearly manifested: his family life, his home, his correspondence. Within this protected sphere, one finds dignity, reputation and, by cross-referring to Article XXIX of ADRDM, also the free development of personality.

8. The spirit of ADRDM and UDHR were infectious in other ways, not only in being of direct inspiration to the ECHR of 1950. May 1949 saw the birth of the Grundgesetz (GG) or Basic Law, which has served as Germany's Constitution to date and which contains a package of provisions which serve cumulatively to protect the private sphere of the individual in ways which are interestingly similar to those of the ADRDM and UDHR. The DGG opens with a statement about the inviolability of human dignity which was, half a century later, no doubt influenced by the German president of the drafting group, taken up almost verbatim in Article 1 CFREU. In its article 2 the DGG echoes Art 22 UDHR when it lays out the over-arching right of unhindered development of personality: "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law." This provision was later to have enormous significance for the development of privacy and data protection law in Germany and indeed across Europe and beyond. The DGG then goes on to protect family life in Article 6, the inviolability of the home in Article 13 and explicitly "the privacy of correspondence, posts and telecommunications" in Article 10. The DGG Article 2 provision on personality came most spectacularly into its own in the landmark Census case of 1983 (https://freiheitsfoo.de/census-act/) where the so-called "General Personality Right" (*Allgemeines Persönlichkeitsrecht*) was interpreted by the BVerfG to also comprise the individual's right, ensuing from the concept of self-determination, to autonomously decide, when and within which limits personal life circumstances are revealed. The term "informational self-determination" (*informationelle Selbstbestimmung*) has been the subject of intense debate ever since, as well as a failed attempt to insert it into the CFREU at the time of drafting. The timing of the 1983 Census decision was also, albeit unintentionally, very significant in the development of the constitutions of several other countries: when the Iron Curtain came down in 1989-90, the concept of free development of personality found itself into the freshly-minted constitutions of several countries newly freed from the Soviet communist yoke. German influence is manifest in the constitution of Romania and Bulgaria to name but two former Eastern bloc states which were careful to explicitly include provisions on development of personality and privacy into their constitutions

9. The right to privacy in German law continues to be directly linked to a series of landmark decisions of the German constitutional court which directly build on the 1983 census decision. These include[3]:

(a) the establishment of an "IT Privacy Right" in response to a state law which provided rather comprehensive rights to certain public authorities including the use of "spyware" to secretly access an individual's information technology systems, search data stored on those systems and monitor online communications. On 27 February 2008, the BVerfG[4] annulled provisions of the North-Rhine Westphalian Act on the Protection of the Constitution, which allowed the government to conduct online surveillance of personal computers. The court ruled that the provisions were unconstitutional as they did not sufficiently respect the individual's right to confidentiality of data stored on information technology systems and the integrity of information technology systems themselves.

(b) the prohibition of the automatic recording of car number plates in March 2008[5]

[3] The BVerFG delivers so many important decisions that relate to privacy that space considerations here restrict us to a tiny handful or representative judgements. A search on automatic recording of number plates alone returns at least four decisions as may be seen at https://www.bundesverfassungsgericht.de/SiteGlobals/Forms/Suche/EN/Expertensuche_Formular.html?input_=5403340&csrftoken=EB0CAD43353BF20BAA73C29FCA6FC705&submit=send&resourceId=5403352&resultsPerPage=50&templateQueryString=automatic+recording+of+number+plates&pageLocale=en.

[4] BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07 -, paras. 1-333, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html.

[5] BVerfG, Urteil des Ersten Senats vom 11. März 2008- 1 BvR 2074/05 -, Rn. 1-185, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/03/rs20080311_1bvr207405.html.

(c) the requirement of proportionality in Telecommunications data retention 2 March 2010[6]

(d) the enforcement of privacy guarantees under the GG being for everybody around the world and not just for German citizens. In its decision in the BND Act Case[7] issued on 19 May 2020, the court ruled that German state authority is bound by fundamental rights; this binding effect is not restricted to German territory. The protection afforded by individual fundamental rights within Germany can differ from that afforded abroad. The Federal Intelligence Service must conform their conduct to the commands of the GG even when their signals intelligence operations only involve foreigners in a foreign context **(**outside of German soil, "foreign-foreign" signals intelligence). This judgement, is a shining example of good practice to all Governments of UN member states and one which reflects the consistent recommendations of the Special Rapporteur on the right to Privacy since 2016 i.e. a person's privacy rights do not and should not depend on the passport carried in one's pocket.

(e) Restrictions on access to on-line data by police[8]

10. The analysis above has been included here to demonstrate that the right to free development of personality and its link to the conceptualisation of privacy as developed by Germany were not born in a vacuum. They were born at the confluence of international thinking on Human Rights and indeed were not first articulated in Europe but rather in the Americas[9]. The international nature of these rights being firmly established, it is however fair to say that Germany has done more than any other country to develop and implement these rights at the national level. Seventy-three years down the line, the right to free development of personality and privacy are solidly and, one hopes, irrevocably part of the German value system. Values no doubt reinforced by the grim remembrance of the gross invasions of privacy endured by millions of German citizens during the existence of the German Democratic Republic (DDR). In terms of privacy, modern Germany is what most other states should aspire to become precisely because the DDR of 1949-1990 is what ALL other states should be working hard to avoid.

11. The right to free development of personality as protected by the Universal Declaration of Human Rights in Articles 22 and 29 and as explicitly linked to privacy by the UN Human Rights Council [10] is thus, today explicitly articulated in German law. Discussion of "personality rights" in Germany has been the most extensive in any UN member state. Thanks to a stream of consistent decisions handed down by the German Constitutional Court since 1983, Germany easily holds the first place out of 193 UN member countries in gradually developing the right to free development of personality. Like it or not, every German Government, of whatever political hue, has to do its best to comply with the standards set by the BVerfG. In the end however, the result can be characterised as a healthy one which reflects healthy tensions inside German society.

---

[6] BVerfG, Judgment of the First Senate of 2 March 2010 - 1 BvR 256/08 -, paras. 1-345, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html.

[7] BVerfG, Judgment of the First Senate of 19 May 2020 - 1 BvR 2835/17 -, paras. 1-332, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html;jsessionid=7D7AC498B8AA2392F473BBE09C58195D.2_cid386 and https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html.

[8] BVerfG, Order of the First Senate of 27 May 2020 - 1 BvR 1873/13 -, paras. 1-275, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200527_1bvr187313en.html.

[9] One of the ironies of life is that the bulk of the text of the Bogota declaration was drafted by US public servants yet the explicit uptake of the doctrine of free development of personality by the United States of America since 1948 has been relatively modest, some would say minimalistic in the extreme.

[10] Resolution 34/7 adopted by the Human Rights Council on 23 March 2017.

A. Legislation regarding surveillance

12. While the Special Rapporteur's mandate has presented a draft legal instrument on government-led surveillance to the UN Human Rights Council in March 2018 and this may be used as an interim benchmark, there is as yet no universally agreed international binding multilateral treaty regulating such matters. UN member states have therefore been very much left to "do their own thing" on safeguards and remedies in the case of state-led surveillance. Germany's approach to this subject reflects a genuine concern to get to grips with the thorny problem of effective oversight of surveillance. The Federal Republic of Germany remains one of a select group of possibly less than 13 countries (of 193 UN member states) which have made serious attempts to address issues of adequate oversight of surveillance following the Snowden revelations of 2013 and since.

13. Since the Snowden revelations, Germany has made progress in various aspects of its oversight system. The most important ones as at November 2018 are the following summarised by the *Stiftung Neue Verantwortung*:

(a) It provides a legal basis for the BND's (Federal Intelligence Service) signals intelligence practice.

(b) Provisions on *ex ante* authorisation and *ex post* control provisions, make it possible to challenge the legality of surveillance measures based on the principles of legality and necessity.

(c) BND's cooperation with foreign intelligence partners are now regulated in detail, obliging the BND to obtain written agreements with its partners aimed at providing safeguards for the legality of the surveillance activities. Additional safeguards include rules on joint databases, where the data provided by the BND will be reviewed by the German Federal Data Protection Authority when the database is managed by the BND. Rules for joint databases and co-operation with foreign partners have equally been amended with regard to the BfV.

(d) The reformed law on the BND requires additional documentation and accountability measures for **t**he Chancelloery's or the Head of the Chancelloery's steering of signal intelligence measures. For example, interception orders must refer to telecommunication nets determined by the Chancelloery. Using selectors that target EU institutions or Member States requires prior notification to the Chancelloery and signal intelligence agreements as and joint databases must be authorized by the Chancelloery. Therefore, the reform facilitates the executive power's accountability over the activities of its intelligence services.

14. The above progress however is only relative up to November 2018 and must be re-measured in the context of the May 2020 decision by the BVerfG cited previously in this report.

15. In November 2018 Special Rapporteur commended:

(a) The general increase of resources for oversight mechanisms that Germany has introduced since 2013 to establish a higher level of protection

(b) The new oversight bodies established since 2013, such as the Independent Body and the Permanent Representative (PR) to the Parliamentary Control Committee (PCC). The G10 Commission has been granted additional investigative competence and the PCC staff has been expanded to 30 members

(c) Arbeitsgruppe 22 within the Office of the Data Protection Commissioner, which is responsible for intelligence oversight, had by end 2018 increased personnel, growing from 6 to now 18 members. Besides the improvement on the quantity of overseeing agencies and personnel, the capacity has also increased due to a greater mix of professional disciplines being available, that is, legal combined with the necessary technical expertise and law enforcement and intelligence experts, as well as from the military

16. In the 28 months or so since November 2018, the mandate of the Special Rapporteur on Privacy has maintained very close scrutiny over developments in Germany and has therefore produced new sets of recommendations and conclusions in Section III below.

B. Surveillance

Levels of surveillance.

(a) Surveillance via closed circuit television (CCTV). Koln as a case-study

(i) At end November 2018 the Police CCTV system consisted of 44 surveillance cameras in total; 25 cameras at the square around the cathedral (17 Multi-focus and 8 PTZ) and 19 cameras in the ring area, the main nightlife spot in the city (13 Multi-focus and 6 PTZ). Sensitive areas in the pictures such as private houses and apartments are pixeled out. The footage is deleted after 14 days. The Police also does not have access to third party cameras such as those of transportation companies. Furthermore, it is reassuring to observe that the Police cameras are connected through a closed circuit ensuring a higher standard for IT security.

(ii) The footage taken can be entered into criminal trials as formal evidence. When the programme started, 85 cases out of 249 (34%) police deployments ended up being used in court. Up to end November 2018, the number arose to 164 cases out of 323 (51%) police deployments. The camera systems do not have facial recognition technology on board and for the near future that is not on the Police's agenda. The next step, which is currently under review, will be to apply movement recognition and recognition of odd movement behaviour.

(iii) The officials spoken to during the Rapporteur's visit to Cologne Police were aware of the potential impact of CCTV surveillance on the right to privacy and stated that it has been developed and is operated with due regard for all data protection and privacy concerns. From a very early stage the Police worked closely with the DPC of NRW on all data protection matters arising from the CCTV project. Before the decision on the use of CCTV was made, the Police consulted the DPC for their expert opinion. The project was then designed accordingly and in each step of the ensuing process the DPC was involved. Importantly, the IT security concept stipulates that the CCTV be carried out in a closed loop. Furthermore, only the criminally most sensitive locations such as the area around the cathedral and the Ring area were under surveillance, and visible parts on the camera like private apartments were pixeled out. Facial recognition software has not been put in place. The authorities assured the Rapporteur that the CCTV surveillance has found large acceptance in the public (although he was not provided with an indication of the tangible evidence supporting this statement).

(iv) As an indication of the precautionary approach to facial recognition in Germany, it was pleasing to be told by the Cologne Police that there are no plans to connect its CCTV system to live facial recognition systems due to the privacy implications. The Rapporteur was advised that future plans might include the use of facial recognition to allow monitoring of the movements of people in the surveyed area but not their individual recognition

(b) Pioneering facial recognition test areas at Berlin Südkreuz Station

(i) The Federal Ministry of the Interior advised that it recently tested facial recognition technologies, using cameras of the German railway system. Only volunteers who had consented to the test were used for the pilot. The Federal Commissioner has pointed out to the Ministry that a pilot is allowed but there is currently no legal basis for facial recognition. The Rapporteur notes that it may be difficult to create a legal basis that is compliant with the Constitutional law particularly with regard to the Persönlichkeitsrecht (Article 2 § 1 and Article 1 § 1).

(ii) Given its great potential impact on the right to privacy, The Rapporteur lauds efforts to thoroughly test the technology before it is deployed. By connecting several systems

consecutively, the Federal Ministry of the Interior states that it managed to reduce false positives to 0.00018%.

(iii) Asked about the kind of situations that the Ministry considers may warrant the deployment of facial recognition technology, its representative said they might use it to search for people suspected of having committed severe felonies. While it may seem premature to conduct such an assessment, proportionality would also depend on whether the search is conducted in a specific location or whether any search would use cameras stationed throughout Germany, potentially infringing the right to privacy of the whole population.

C. Surveillance for purposes of law enforcement

17. Law enforcement agencies in the Länder are responsible essentially for crime prevention and crime prosecution. There are special departments for police state protection in the state criminal investigation offices. Since the police do not have access to the databases of other security authorities, they must take their own measures to fulfil their tasks. The exchange of information among security authorities is an essential part of this task fulfilment. This exchange is subject to a legal framework. The executive police officers constantly fulfil their obligation to cooperate with the Data Protection Commissioner (DPC) of their authority. The police are obliged to cooperate with the Data Protection Commissioner.

18. This close cooperation between the DPC and the Police preceded the adoption of the GDPR. Therefore, many of the new data protection obligations were in place already. However, some problems have arisen in regard to the concrete transposition of European law into German law, for example, when carrying out privacy impact assessments. When it comes to the evaluation of the quality of the data, there are still improvements to be made.

19. Across the Länder, data protection supervision is divided into two bodies: the Landesdatenschutzbeauftrager (Commissioner for Data Protection) who is responsible for public sector bodies and the Landesamt für Datenschutzaufsicht (State Office for data Protection supervision), which is responsible for private sector bodies.

20. Some of the officials in the office of the DPC responsible for Police oversight have a Police background which is not perceived as a problem.

21. Moreover, in some areas such as Bavaria, automated electronic data file require, prior to conception, a creation decision (“Errichtungsanordnung”). This type of decision must include amongst other matters, the purpose of the file, prerequisites of the storage, transmission and use, accessibility, time limitations and has to be permitted by the Bavarian State Ministry of the Interior (cf. e.g. Article 64 BayPAG). An authorisation by the Landes DPC is not required, just a notification.

22. The competences of the Länder DPCs mirror the competences of the Federal DPC. Their main task is to fulfil the duties laid down in Article 57 of the GDPR as well as to advise and provide recommendations to the law enforcement, security and intelligence agencies with regard to data protection law. The The Federal and the Länder DPCs are elected by the Federal resp. Land Parliament for at least 4 years period of eight years and have to possess the qualification of judgeship or an equivalent qualification (e.g. Sec. 11 Federal DP Law; Sec. 25 § 1 S. 4 DP Law NRW). The DPC has access to all premises of the agencies as well as to their electronic databases e.g. (Sec. 16 § 4 Federal DP Law; Sec. 27 § 2 S. 2 DP Law NRW).

D. Surveillance for purposes of national security (domestic/foreign surveillance)

23. The Bundesamt für Verfassungsschutz as a federal security agency coordinates the co-operation of the agencies of the Länder (Sec. 5 §3 S.1 BVerfSchG), including the establishment of common rules to ensure the ability to cooperate, the general work focus and work sharing as well as the criteria for the common data bases under Sec. 6 BVerfSchG (cf. Sec. 5 § 3 S. 2 BVerfSchG). However, it has no competence to give direct instructions or control the agencies of the Länder on individual measures. To a limited extent, the federal

agency can set up basic frameworks which are followed by the agencies at Land level (Sec. 5 §2 S.2 BVerfSchG). Further there is a common database called "NADIS" in order to effectively exchange information between the different security agencies at the Federal and Länder levels. Law enforcement agencies do not have access to this system. All in all, the 16 Länder agencies are generally separate from each other.

24. In order to ensure a measure of coordination over the 19 security agencies in Germany as well as over the 20 law enforcement agencies, certain coordination centres have been set-up. The Joint Counter-Terrorism Centre (GTAZ) was established in 2004. According to the German authorities, a special legislative authorisation was not required as the centre does not possess any competences of its own.

25. Another centre was established in 2012 – the Joint Counter-Extremism and -Terrorism Centre (GETZ). It mainly focuses on counter-extremism and reunites more than 40 law enforcement and security agencies. While these centres have set-up shared databases, access to the information in these databases differs between law enforcement and security agencies.

26. The Antiterrordatei (cf.Sec 1 § 1 ATDG) is an example of such a database and works as an index system. An agency does not gain full access to all information in the database but only the information it has supplied. If an agency seeks access to information held by other agencies, it must identify another agency who has that information and contact it to seek access. In the case of more sensitive information, it is possible for the agency inserting the information in the database to make that information "invisible".

27. Should another agency seek information on that particular person, the agency which possesses this information will receive a message advising another authority has been searching for it and the agency who holds the information can decide to respond and to volunteer the information. Only in rare cases, when a threat is imminent, can all the relevant information in that database be queried directly. In this case, the principle of informational separation prevails unless there is an imminent threat to the state.

28. The Police, therefore, generally have to collect information and cannot rely on information collected by the security agencies, however, in certain conditions, the Police can have access to information in the Antiterrordatei, and provide information to it.

29. Unlike the Austrian security service, the prevention of terrorism as such is not a legally defined task of the security agencies, but terrorism is observed as a special form of extremism because it usually threatens or attacks the free democratic order. Organized crime is also not always covered by the security services. Some Länder, such as Bavaria, Hesse and Saarland, do integrate organized crime into their intelligence portfolio.

30. The security agencies are, according to the government, the most controlled agencies in Germany. Mirroring the situation at the Federal level (see section on oversight below), the secret intelligence agencies are controlled by the Land PCC, the Land GC, the Land DPC and the administrative courts. When intercepting somebody's communication, the GC claims that it rigorously oversees the intelligence agencies and can assess the legality of the measure better than any single judge.

31. The main oversight is, nevertheless, done from an *ex ante* perspective. *Ex post* oversight consists of reporting obligation towards the PCC. The DPC is obliged to carry out a biannual control. Another internal oversight is supposed to be performed by the superior agency such as the ministry for the interior. The relevant minister is also regularly informed about the agencies' activities.

32. Another safeguard is the fact that the ability of requesting the adoption of certain measures lies in a specific department; hence, not all the members of the agencies can equally request surveillance measures.

E. Oversight of agencies carrying out surveillance

33. The Parliamentary Control Committee (PCC):

(a) The PCC consists of nine Members of Parliament. It is supported by the Permanent Representative and his staff. Its core task is to oversee the work of the Bundesnachrichtendienst (BND), Bundesamt für Verfassungsschutz (BfV) and the Bundesamt für den Militärischen Abschirmdienst (MAD).

(b) Its members are elected by the Parliament at the beginning of each legislative term (Sec. 2 § 1 PKGrG). The Parliament decides upon the number, the composition and the functioning of the PCC (Sec. 2 § 2 PKGrG). Meetings are to be held at least every three months. (Sec. 3 § 1 S. 1 PKGrG) and according to the current by-laws at least once per month (Sec. 3 § 1 S. 1 GO PKGrG).

(c) The meetings can also be held inside of one of the agencies (Sec. 3 § 1 S. 4 GO PKGrG). Participants in the meetings comprise the members of the PCC, the Permanent Representative, the staff, and by invitation, other Government officials, such as state secretaries or heads of departments (Sec. 3 § 6 S. 1, 2 GO PKGrG).

(d) The Government is obliged to inform the PCC comprehensively about the general activities of the secret service agencies and about events of outstanding significance, namely major changes in the overview of the situation regarding interior and exterior security, internal activities of the agencies with major significance for the fulfilment of tasks, single incidents which are subject of public debate or public reporting (Sec. 4 § 1 S. 1, 2 PKGrG).

(e) The Government also has to inform the PCC about other events or activities if the PCC wishes so (Sec. 4 § 1 S. 3 PKGrG). The Government has the right to deny access to relevant information for the reasons of access to information (e.g. if a foreign secret service only allows access to information under the condition of non-disclosure to the PCC), protection of personality rights of third persons, protection of executive core area (Sec. 6 § 2 S. 1 PKGrG). A denial by the Government has to be justified (Sec. 6 § 2 S. 2 PKGrG).

(f) The by-laws (GO PKGrG) concretize the activities and events of outstanding significance (Sec. 4 § 1 S. 1 GO PKGrG). Without a definitive and final classification, the following circumstances are enumerated in the annex to the GO PKGrG:

(g) In more general terms: Events and activities that differ from the regular routine of the secret services, that have to come to the attention of the PCC for maintaining an effective control; it is not relevant whether the events have been initiated by the agency itself.

(h) Situational:

(i) Terrorist, military and criminal developments of major relevance that may become a threat to Germany, its population, its institutions and to critical infrastructure;

(ii) Indication of a formation of an anti-constitutional network or group, particularly left- and right-wing extremism as well as foreign terrorism; and

(iii) Activities of foreign authorities and organisations within or against Germany, including any initiated measures.

(i) Organisational:

(i) Internal changes of departments (establishment and abolishment)

(ii) New co-operations of fundamental significance

(iii) Establishment of combined offices

(iv) Introduction of new methods and new instruments of fundamental importance in respect of international cooperation

(v) Criminal offences of members of the agencies and other internal procedures which are likely to impair the working methods, the tasks or the use of authority of the services

(vi) Other internal activities appropriate to impair the functioning, assignment of tasks, or use of the competences of the services

(vii) Single activities that are part of political discussions or public coverage.

(j) In terms of competence, PCC has the right against the secret service agencies and the government to access files, documents as well as data saved in electronic files (Sec. 5 § 1 S. 1 PKGrG) of the security and intelligence services and the government. The PCC is also allowed to access the agency's premises (Sec. 5 § 1 S. 2 PKGrG). The requests by the PCC have to be complied with immediately (Sec. 5 § 3 PKGrG).

(k) The Permanent Representative supports the work of the PCC by carrying out investigations into particular topics on a regular basis (Sec. 5a § 1 PKGrG). The Permanent Representative investigates specific circumstances under the directive of the PCC (Sec. 5a § 2 S. 1 PKGrG). He or she prepares the PCC's meetings and the PCC's reports to the Parliament and he participates in the regular meetings of the PCC, the G10 Commission and the Trustee Board. The PCC proposes a candidate to the President of the German Parliament who then appoints the Representative for a term of 5 years (Sec. 5b § 1 S. 1 PKGrG). A reappointment is only admissible once. Permanent Representative can only be a person of more than 35 years, possessing the qualification of judgeship or is admitted to the German (non-technical) higher administrative service, and who is allowed to handle classified information and sworn to secrecy; he or she must not hold another office or undertake other employment (Sec. 5b § 2 PKGrG).

(l) The PCC can – by a majority of two thirds – employ a (technical) expert (Sec. 7 § 1 PKGrG).

(m) Members of the secret services are allowed to contact the PCC on official matters whenever there is an instance of maladministration. For that the officers contacted must not be reprimanded, penalised or disadvantaged (Sec. 8 § 1 S. 1, 2 PKGrG). In case of a complaint, the government is consulted to comment on the subject matter (Sec. 8 § 1 S. 3 PKGrG). In case of a complaint by a citizen regarding the dealings of the secret agencies with regard to his person directed to the Federal Parliament the case can submitted for the PCC's attention.

(n) The meetings of the PCC are confidential (Sec. 10 § 1 PKGrG). Specific assessments can be released to the public by a majority of two thirds of the present members. The stipulations of confidentiality have to be taken into account;in this case every member is entitled to present a dissenting opinion (Sec. 10 § 2 PKGrG). In addition, the PCC publicly hears the presidents of the security and intelligence services once a year (Sec. 10 § 3 PKGrG).

(o) The PCC is assigned a requisite number of employees of the Administration of the German Bundestag for its assistance (Sec. 12 § 1 S. 1 PKGrG). The Permanent Representative is head of the employees (Sec. 12 § 2 PKGrG).

(p) The PCC must report to the Federal Parliament, at least twice - after each half of the legislative period - on the government's compliance with its obligations and particularly the obligation to report to the PCC in cases of outstanding significance (Sec. 13 PKGrG).

(q) Under the G10 Law, the relevant ministry is obliged to report at least every six months to the PCC the use of any measures according to the G10 Law (Sec. 14 § 1 G10 Law). The relevant ministry can take these measures without the prior authorisation of the PCC if there is an imminent threat. The PCC's president has to be consulted within three days and the full authorisation has to be made up no longer than two weeks after using these measures (Sec. 14 § 2 G10 Law).

34. The G10 Commission:

(a) The G10 Commission (GC) consists of its chairman who must possess qualified judgeship, three members and four substitute members (Sec. 15 § 1 S. 1 G10 Law). All of them have the right to pose questions and make statements during the meetings (Sec. 15 § 1 S. 2 G10 Law).

(b) The members are independent and not subject to instructions or directives (Sec. 15 § 1 S. 2 G10 Law). They are appointed by the PCC after hearing the government for one legislative period and their term ends with the establishment of the next GC, or more than three months after the end of the legislative period.

(c) The meetings are confidential (Sec. 15 § 2 S. 1 G10 Law). The GC has to be provided the necessary personnel and equipment (Sec. 15 § 3 S. 1 G10 Law), with technical experts (Sec. 15 § 3 S. 2 G10 Law).

(d) The GC meets at least once a month (Sec. 15 § 4 S. 1 G10 Law). Its main task is to decide ex officio or on individual complaints about the admissibility and necessity of the measures taken on the basis of the G10 Law (Sec. 15 § 5 S. 1 G10 Law). Its competence of control extends to any kind of processing of personal data gathered by using measures based on the G10 Law and deployed by the federal secret service agencies as well as to the issuing of notifications to affected persons (Sec. 15 § 5 S. 2 G10 Law).

(e) The competence for oversight is not only for the requests, but for the complete process of collection and processing of data (BVerfGE 100, 313, 401). The GC is therefore entitled to receive answers to its questions, to access all relevant documents, stored electronic data, and data processing software, as well as to access all agencies' premises at all times (Sec. 15 § 5 S. 3 G10 Law).

(f) The relevant ministries report monthly to the GC about the measures they intend to take prior to their execution (Sec. 15 § 5 S. 1 G10 Law). In case of an imminent threat, the measure can be taken prior to its authorisation; data may be collected from the day of the request (Sec. 15 § 5 S. 2, 3 G10 Law). However, the data may only be used after authorisation (Sec. 15 § 5 S. 4 G10 Law). In case the authorisation of the relevant ministry is not granted within 24 hours or the GC decides it is admissible under G10 Law, the collected data must be automatically and irrecoverably destroyed (Sec. 15 § 5 S. 5 G10 Law. The measures that do not meet the formal and necessity criteria must be terminated immediately (Sec. 15 § 5 S. 6 G10 Law).

(g) The relevant ministry provides monthly reports to the GC about the notification to affected persons (Sec. 15 § 7 S. 1 G10 Law). In case the GC deems an omitted notification necessary, it has to be issued immediately (Sec. 15 § 7 S. 2 G10 Law).

(h) The GC and the PCC exchange regularly information on general matters regarding their control functions (Sec. 15 § 8 G10 Law).

35. The Independent Panel:

(a) The Independent Panel (IP) consists of a president, two assessors as well as three substitute members (Sec. 16 § 1 S. 1 BNDG). The members are independent and not subject to instructions or directives (Sec. 16 § 1 S. 2 BNDG). The president as well as one assessor are judges at the German Federal Court of Justice; the other assessor is a Federal Prosecutor (Sec. 16 § 1 S. 3 BNDG). The substitutes reflect the same composition as the permanent members (i.e. 2 judges and 1 prosecutor). The members are appointed by the federal cabinet on the proposal of the presidents of the relevant institutions (Sec. 16 § 2 BNDG) for a period of six years. The IP is located at the German Federal Court of Justice (Sec. 16 § 3 S. 2 BNDG).

(b) The IP's main task it to examine the admissibility and necessity of measures on the basis of the BND law (Sec. 9 § 4 S. 2 BNDG):

(c) The Chancelloery reports to the IP prior to the implementation of the relevant measures (Sec. 9 § 4 S. 1 BNDG). Implementation is permitted prior to the report if the objective of the measures otherwise could not be achieved or it would be significantly impeded (Sec. 9 § 4 S. 3 BNDG). In this case, the report has to be made up without further delay (Sec. 9 § 4 S. 5 BNDG). When the IP considers that a measure does not meet the formal and/or necessity criteria, the measure must be suspended immediately (Sec. 9 § 4 S. 6 BNDG).

(d) Regarding the selection of search terms, the Chancelloery reports to the IP if they refer to institutions of the European Union (EU) as well as public institutions of the EU member states (Sec. 9 § 5 S. 1 BNDG). If one of these decisions is declared inadmissible or unnecessary, it requires the immediate termination of the measure in question (Sec. 9 § 5 S. 2 BNDG). The IP can check the compliance of the selection of search terms with the BNDG at any time by a spot check (Sec. 9 § 5 S. 3 BNDG). The same competence exists as to the automated transmission to a foreign public entity (Sec. 15 § 3 S. 7 BNDG).

(e) The deletion of data gained by illegal surveillance also has to be reported to the IP (Sec. 10 § 3 S. 2 BNDG).

(f) The IP has to be provided the necessary personnel and equipment (Sec. 16 § 3 S. 1 BNDG).

(g) The IP meets at least every three months (Sec. 16 § 4 S. 1 BNDG). The meetings are confidential (Sec. 16 § 5 S. 1 BNDG). The IP reports at least every six months to the PCC about its activities (Sec. 16 § 6 BNDG).

36. The Federal Data Protection Commissioner:

(a) The Federal Data Protection Commissioner (DPC) is elected by the Federal Parliament on proposal of the government for a term of five years; re-election is possible once. The office numbers 251 members in Bonn and Berlin. The current DPC is Ulrich Kelber. The DPC acts independently and is only bound by law.

(b) The main tasks of the DPC are:

(i) Ensuring compliance with the General Data Protection Regulation (GDPR) and Directive 2016/680 as well as the Bundesdatenschutzgesetz (BDSG);

(ii) Awareness raising;

(iii) Advising the parliament and other public institutions with regard to data protection;

(iv) Processing of complaint by affected persons;

(v) Cooperation with foreign data protection agencies;

(vi) Oversight.

(c) Insofar as the security and intelligence agencies as well as law enforcement agencies are concerned, the DPC acts as an oversight body only as far as this function is not exercised by a specialized body such as the GC (e.g. Sec. 26a § 2 BVerfSchG; Sec. 26a § 3 S. 1, 2 BVerfSchG). In pursuing this task, the DPC has the right to receive explanations, as well as access to all relevant files and access to the agency's premises (Sec. 16 § 4 BDSG). These rights can be restricted if the Ministry for the Interior identifies a certain threat for the security of the state or the Land (Sec. 26a § 3 S. 3 BVerschG).

37. General concerns about oversight of surveillance

(a) While some improvements of the oversight mechanisms in Germany have been identified above, it must be acknowledged that Germany's intelligence oversight is still far from comprehensive and fully effective:

(i) The first problem concerns the continuous and further expanding fragmentation of the intelligence oversight. This is not only the result of Germany's federal structure. Albeit the German system might appear to be a fine-tuned system *prima facie*, it is very unclear as to how well it works and how suitable it is to deal with current threats of abuse.

(ii) Cases from other countries such as the UK show the blunt fabrication of information by intelligence agencies uttered to the relevant oversight bodies. Germany has no fully suitable mechanism that could securely prevent or at least detect such abuse. There is no independent – but necessary- mechanism in place that addresses the issue.

(iii) In November 2018 the Special Rapporteur pointed out that another problematic aspect introduced by recent legislative reforms is the fact that the Federal Intelligence Service Act offers a weaker level of protection for the right to privacy of non-EU citizens. In general, German authorities are bound to their obligations foremost in terms of the *Allgemeines Persönlichkeitsrecht* (Article 2 § 1 and Article 1 § 1) irrespective of the nationality under Germany's jurisdiction. According however, to the then-current rules on the communication intelligence of foreigners (non-EU citizens) abroad,

a discrimination is allowed. Sec. 6 § 1 BNDG specifically allows the processing of data – under specific circumstances – of foreigners abroad. In addition, the use of search terms that specifically refer to EU institutions, EU member states as well as EU citizens is only allowed under very particular circumstances (Sec. 6 § 3 BNDG). This discrimination based on nationality is clearly incompatible with Germany's international law obligations and, following the Special Rapporteur's visit in November 2018 has also been declared unconstitutional by the BVerfG. This thinking is consistent with the logic wherein there is no reason to distinguish between foreigners abroad and non-foreigners abroad. The International Covenant on Civil and Political Rights, ratified by Germany on 17 December 1973, obligates the Government to ensure to all persons all human rights recognized in the Covenant, including the right to privacy (Article 17), without distinction of any kind.

38. Some concerns specifically related to federal status and historical context:

(a) Germany is a federal state. It is made up of16 "Länder". The competences are distributed according to Articles 70 et seq. German Constitution. With regard to the Republic of Weimar, the current constitution seeks to ensure that the competences for crime prevention and the Police are not assigned to the Federal Government but to the Länder. The same applies to the security services, which act as threat prevention institutions and responsibility is therefore also located at Länder level.

(b) As soon as a threat affects not only one Land but Germany as federal state, the competences must also lie on the federal level in order to effectively prevent any threat.

(c) Another important element in German law regarding the activity of law enforcement, security and intelligence agencies is that they are strictly separated (principle of separation). This principle as such is nowhere to be found in the constitution in an explicit way, yet some scholars derive it from Article 87 Constitution. For others it follows from the overall Rechtsstaatspinzip or directly from the basic rights. This principle goes back to the "Polizeibrief" of the Western Allies of 14 April 1949 and is well established in statutory law (e.g. Sec. 8 § BVerfSchG).

(d) The Federal Constitutional Court in various decisions (e.g. BVerfGE 100, 313 – "Telekommunikationsüberwachung I") has mentioned it, but the question has never been clarified. The principle of separation requires an organizational separation and also the prohibition of assigning enforcement powers to the security and intelligence agencies. According to German law, security and intelligence agencies are only responsible for gathering intelligence, not for its enforcement.

(e) A more difficult aspect concerns the sharing of certain information. According to the Federal Constitutional Court, the sharing of data is not illegal as such and can be justified in certain exceptions (cf. BVerfGE 133-277 **"**Antiterrordatei").

(f) The problem arises from the rule that data must be strictly used only for the original purpose for which it has been collected. Whenever a chance find occurs for the intelligence agencies, it generally must not be shared with the Police for preventing, investigating and initiating further prosecution for a different crime.

(g) Under certain conditions the change of the purpose for data collection and processing however, is allowed only if certain conditions are met:

(i) the change of purpose is lawful,

(ii) necessary to protect an overall interest of society, and

(iii) proportionate to the protected interests of the constitution (BVerfGE 141, 220; 100, 313; 65, 1).

39. Overall Situation in the Länder: Examples of Bavaria and North Rhine-Westphalia:

(a) The basic structure of the oversight mechanisms including the roles of the Data Protection Commissioners of the Länder is generally comparable to what can be found at the federal level.

(b) It is yet unclear however, whether the available resources of the relevant Data Protection Commission Offices are sufficient. The number of people working for the Data Protection authority indicates a significant inadequacy with regard to the population within Bavaria as well as North Rhine-Westphalia. Furthermore, the composition of the oversight authorities is yet to be reformed to include information technology specialists.

(c) Therefore, some Länder have adapted their laws to actually receive foreign intelligence on other aspects such as organised crime. The competence to react to organised crime is not a competence that is shared amongst all of the Verfassungsschutz agencies in the Länder. Bavaria is an example (cf. Article 3 S.2BayVSG).

F. Export control

40. The Special Rapporteur learnt with concern that, according to media and NGO reports that surveillance software at least partially developed in Germany by Finfisher GmbH, had been used to commit human rights violations in several countries, including Bahrain, Egypt and Turkey.

41. When asked, the German Government stated that Germany had not granted any export licences to Finfisher. A license to export its software, would have been required by the law in order for the company to be able to export its products to governments outside of the EU, or to another EU country with the intent of exporting it to a third country.

42. In November 2018, the German Government did not reveal whether law enforcement/judicial authorities are carrying out any investigations of the allegations, or whether it intends to prosecute the company for violation of export regulations. The Special Rapporteur notes however that in October 2020 the German Customs Investigation Bureau (ZKA) searched 15 residential and business premises in Germany and abroad with connections to the Munich-based surveillance software firm FinFisher.

G. Privacy laws not directly concerned with government-led surveillance including Health-related data

43. Germany possesses one of the most up-to-date and comprehensive regulatory systems for privacy and data protection, having implemented the currently highest international standards i.e. those established in the EU's GDPR and the Council of Europe's Convention 108+.

III. Conclusions and Recommendations

A. On intelligence oversight, security and surveillance

44. **The Special Rapporteur commends all efforts in Germany to meet the standards set by the BVerfG and additionally uses this opportunity to make some observations and recommendations about the new law on surveillance and oversight published on the 16 December 2020**[11]**.The BND law (already in the version of December 2020) establishes one unified new control authority (Unabhängiger Kontrollrat, Independent Supervisory Council (ISC)) consisting of the quasi-judicial control organ and the administrative control organ. The ISC will be reporting to the PCC.**

(a) **While the Rapporteur commends the positive innovations e.g. Sec. 19 point 5 in combination with Sec. 20, par. 21 and Sec. 22 of the draft surveillance law), he raises some concerns with special procedures which are envisaged for metadata**

[11] Ministerial draft of the Federal Chancelloery - Draft law amending the Federal Intelligence Service Act to implement the rulings of the Federal Constitutional Court and the Federal Administrative Court partially entered into force on 22 April 2021, the rest will enter into force on 1 January 2022. https://data.guardint.org/en/entity/olcnshnohe?file=1613469427577z9cuqu3vct.pdf&page=1.

being kept completely sealed within the premises of the German intelligence agency (BND). The Rapporteur recommends that supervising bodies shall have equal access to them so that they can better exercise their powers and fulfil their functions.

(b) **In contrast to the current draft proposals, the Rapporteur recommends that no distinction is made between metadata and other personal information and that these be treated equally at all stages of collection and processing, irrespective of whether the processing is automated or performed by a human agent;**

45. **In his analysis of the draft surveillance law[12] the Special Rapporteur endorses those views expressed in the public domain to date[13] which identify:**

(a) **the problem of overlapping and vague competencies of the supervising authorities;**

(b) **the need for reinforcement of the supervisory role of the independent administrative body;**

(c) **the need to specify the accountability obligations of surveillance bodies;**

(d) **the need to strengthen and expand the evaluation of the oversight mechanisms;**

(e) **the need to reinforce the independence of the supervising authorities;**

(f) **the need of oversight bodies to exchange and cooperate with one another;**

(g) **the need for simplification and final general observations on the oversight scheme**

46. **The Special Rapporteur shares the concerns expressed by Germany's Federal Commissioner for Data Protection & Freedom of Information when he warns that:**

> ***"The draft BNDG on many aspects does not meet the proportionality requirements set by the Federal Constitutional Court for strategic foreign surveillance of telecommunications and transfers of data obtained through it to other domestic and foreign intelligence and law enforcement authorities. Likewise it is doubtful whether the provisions for CNE-data collection and transfers introduced by the current BNDG draft meet the requirements set in precedents by Federal Constitutional Court, in particular its rulings on access to information technology systems by intelligence and law enforcement authorities. In order to avoid the risk of further successful constitutional complaints, the mentioned shortcomings of the draft BND should be remedied. In addition, the supervision needs to be strengthened in a way which allows for an unrestricted content related and effective cooperation between the current and future supervisory bodies for the BND."***[14]

47. **In summary, the Special Rapporteur recommends that the German Government consider the following package of measures pertinent to all reforms of surveillance laws:**

(a) **the powers of the general administrative authority shall be provided for by law in a detailed manner including, at minimum, competences with regard to:**

(i) **the adequacy control of the suggested surveillance measures (par. 24 of the draft law),**

(ii) **the collection and storage of metadata,**

(iii) **the documentation of the processing activities on metadata;**

(iv) **the power of the general administrative authority to appeal against surveillance measures provided for in par. 52 of the draft law, shall be**

[12] *Ibid*.

[13] Eg. Ulrich Kelber, Aspects where Germany's draft Federal Intelligence Services Act misses the mark, https://aboutintel.eu/bfdi-on-bnd-shortcomings/.

[14] Ulrich Kelber, Aspects where Germany's draft Federal Intelligence Services Act misses the mark, https://aboutintel.eu/bfdi-on-bnd-shortcomings/.

further specified, especially with the aim to clarify the procedure and, most importantly, the maximum time delays allowed to the intelligence services for response;

(b) **the independent administrative authority should be awarded the following four additional powers:**

(i) **the power to oversee more surveillance activities than the ones currently available to it according to par. 42 of the draft law,**

(ii) **the power to check for compliance *ex ante*, before each surveillance measure is undertaken, which currently is not available to it,**

(iii) **the strengthening of its enforcement abilities and the ability to impose sanctions, as it currently lacks any effective remedies against controversial surveillance measures and**

(iv) **the ability to oversee all the search terms inserted by intelligence agents.**

(c) **The provisions of par. 55 point 1 of the draft law, requiring the administrative authorities exercising oversight duties to report to the special parliamentary committee every six months should be amended to a minimum three monthly reporting cycle, and expanded such that the law shall prescribe in more detail the exact issues on which the oversight authorities shall report, thus increasing clarity and transparency;**

(d) **The oversight procedure should envisage the participation of federal judges with carried out in an adversarial fashion enabling all possible opinions to be presented, analysed and evaluated.**

(e) **Provisions on the co-operation between oversight authorities should be more detailed containing precise regulation on the frequency, duration, agenda, content and ultimate goal of multiagency cooperation between all the oversight authorities.**

48. **Whether provided for in one law or several:**

(a) **The structure and interplay of the oversight agencies should be simplified with consideration given for oversight of all types of surveillance, irrespective of whether this is carried out by Federal state agencies, whether intelligence or law enforcement, being consolidated within a maxim of two entities. When doing so, Germany should do its utmost to ensure that *a posteriori* inspection is not carried out by the same body which granted *a priori authorisation* of surveillance;**

(b) **The German authorities competent for the use of bulk powers for surveillance first examine, then determine priorities and adopt to the greatest possible extent, the measures required for introducing the good practices identified in the compendium published by *Stiftung Neue Verantwortung* on 08 November 2018.**

(c) **That Germany's independent oversight authority/ies have technical systems in place such as a secure room with direct access/interface to the IT systems of Law Enforcement Agencies (LEAs) and Security and Intelligence Services (SIS) from which independent external oversight can be exercised at will without prior notice being given to the LEA or SIS concerned;**

(d) **That any members of the German Judiciary expected to take part in the decision making related to surveillance, receive adequate training to enable them to better understand the nature of the technologies that they are regulating and the possibly far-reaching consequences of their actions;**

(e) **That where Germany shares personal information and/or intelligence product with other countries it ensures that it installs or reinforces adequate privacy safeguards in place for those occasions where such sharing of information/intelligence product occurs.**

B. On privacy and health-related data

49. **The COVID-19 pandemic has provided an opportunity for reflection. Most, if not all, of the issues raised by wearables, computerisation of health records, related use of artificial intelligence, technology applications in contact-tracing and standards to be respected, even in a pandemic, are addressed by the Special Rapporteur's recommendations on the subject as explained in the accompanying Explanatory Memorandum. The Special Rapporteur therefore respectfully draws the attention of the Government of the Federal Republic of Germany to the Recommendations on the protection of Health Data which he presented to the General Assembly of the UN in October 2019. He also urges the German Government to reflect about the successes – and failures – in attempts to use applied technologies and especially smartphone apps in attempts to fight the COVID-19 pandemic.**

C. On gender and privacy

50. **During the course of his visit the Special Rapporteur could observe instances when gender could impact the way that privacy is experienced. The Special Rapporteur therefore respectfully draws the attention of the Government of the Federal Republic of Germany to his findings and Recommendations on Gender and privacy, which he presented to the UN Human Rights Council in March 2020**[15] **The principles outlined therein should be closely respected and implemented.**

D. On big data analytics, open data, children and privacy

51. **The Special Rapporteur respectfully draws the attention of the Government of the Federal Republic of Germany to his findings and Recommendations on Big Data and Open Data, and the Recommendations on Gender and Privacy which he presented to the UN General Assembly in October 2018**[16] **and October 2017**[17]**, as well as his findings and recommendations to the Human Rights Council on Privacy and Children in March 2021**[18]**.**

E. On Germany's role on the international stage

52. **The Special Rapporteur has noted a number of international statements by the Government of the Federal Republic of Germany on the subject of encryption and concerns expressed about such matters**[19]**. He again directs the attention of the German Government to the identification of relevant risks outlined in the paper published by the Government of the Kingdom of the Netherlands on 04 January 2016. The Special Rapporteur sees the Federal Republic of Germany as being especially well-positioned to take a leadership role in building bridges within the EU, across a wider Europe, and with the USA and other democratic countries around the world in matters concerning privacy, encryption and surveillance.**

---

[15] https://undocs.org/A/HRC/43/52.
[16] https://undocs.org/A/73/438.
[17] https://undocs.org/A/72/540.
[18] https://undocs.org/A/HRC/46/37.
[19] See for example: *The Encryption Debate in Germany: 2021 Update* published 31sMarch 2021, https://carnegieendowment.org/files/202104-Germany_Country_Brief.pdf.